1. Lecture 1 (6.10.11)

We give a glimpse of some of the important notions/buzzwords that will be studied in the course.

1.1. **The notion of divisibility.** One of the most important notions in (elementary) Number Theory is the one of divisibility. Given a natural number n (i.e. $= 1, 2, 3, \dots$), can we divide them into, say, k parties evenly? Or, more generally, when can one lay out n objects of the same kind and size evenly spaced in a rectangle? Eg for $n = 15$, we can find a rectangle of the form 3×5 in which we can place our 15 objects neatly. In a sense, such a number like 15 can be thought of as occurring also as a "2-dimensional" size. If $n = 17$, say, this is not possible–what about $n = 323$ or $n = 691$?

1.2. **Primes = building blocks for divisibility.** Numbers for which the latter is not possible (i.e. which only occur as a "1-dimensional size") are called *primes*–we exclude the number 1 here. These play a crucial role in number theory as they are the building blocks of sorts for the set of numbers (multiplicatively speaking, see below).

1.3. **Detecting primeness.** There seem to be no easy patterns among integers which guarantee primeness, and one can easily misjudge the corresponding nature, i.e. being prime or not, of an integer—even one of the best Number Theorists of his time (Pierre de Fermat 1601–1665) fell into the trap: he saw a "prime pattern" in the following sequence 2, 3, 5, 17, 257, 65537 (all of which are indeed prime) and guessed that this prime property would hold for each sequence member. But about a century later Euler (another NT hero) found a factorisation of the very next number in this sequence.
(Q: which is it? A: $4294967297 = 2^{2^5} + 1$, divisible by 641 and 6700417.)

But at least there are very efficient tests (*primality tests*, of which we will encounter one or two) which check reasonably fast whether a number is prime or not–without having to determine *any* of its prime factors!

1.4. **Fundamental Theorem of Arithmetic: existence and uniqueness of such a decomposition.** It turns out that each natural number can be written as a product of primes, i.e. we can "decompose" or "factorise" such a number into building blocks. What is more, this decomposition into primes not only exists, there is only one way to do this—the prime factors involved are uniquely determined, as well as how often they occur. This fact is a very basic one, reflected by the name of the corresponding theorem, the "fundamental theorem of arithmetic". One could argue that this is one of the reasons why divisibility is such a powerful notion.

And just to caution you: such a uniqueness of factorization is far from the norm in slightly more general contexts (e.g. in so-called "number rings").

1.5. **Realising such a decomposition.** How about actually achieving a factorization? Nowadays such a factorisation of a 10-digit number on a computer is instantaneous, even finding the factorization of a number up to 100 digits, say, takes only a few minutes on a standard computer. But even now if we want to achieve the same for a 200-digit number we are often out of luck!

1.6. **Cryptography from discrepancy.** Now suppose we find two huge primes, of about 100 digits each, then it takes a computer an instant to multiply them together but it is in most cases practically impossible for someone else to decompose (of course with the help of a computer) the result back into a product of primes. This amazing incongruence between easy "operation" (here multiplication) and hard "reverse operation" (i.e. factorisation) is actually used in cryptography in everyday life situations like secure data transmission or Internet banking etc.

But in order to understand what is behind this, we first need to get a good grip at the divisibility properties of the integers. On the other hand, we will also need to get a feel for how to encrypt messages and, more importantly, how to encrypt things publicly/in broad daylight (so-called *public key cryptography*) in such a way that only someone with "extra knowledge" can actually decrypt it (without sneaking into the drawer/trash can of the sender, of course).

1.7. **How many primes?** Back to our building blocks: an immediate question is whether there are enough such primes at all; we will soon see that there are in fact infinitely many such. But proofs of this fact are "qualitative" in nature; in fact, so far no-one has ever found a closed formula which produces infinitely many primes, and primes only. Also, we will discover a sensible way to ask "how many" primes there are, which is the content of the famous prime number theorem (an analytic result which we will not prove, stating that the number of primes below a bound x is roughly of size $x/\log(x)$).

1.8. **"Comparing divisibilities".** One further feature of divisibility will be prominent soon: while it can be very hard to decompose a given integer, it is in contrast very fast to "compare divisibilities" of two integers with each other, i.e. finding common divisors if they exist. This goes back 2000 years to Euclid, and the resulting (Euclidean) algorithm is the prototype of a fast and efficient algorithm.

1.9. **Working with congruences.** Divisibility naturally groups integers into classes: two integers a and b are considered indistinguishable (*congruent*) with respect to a chosen natural number n if their difference is divisible by n, i.e. if they leave the same remainder when dividing by n. In this vein, it makes sense to think of all the multiples of n as being zero! It turns out that this notion of being congruent is perfectly compatible with most of the ways we commute with the integers normally, leading to a "calculus of congruences". In fact, we are quite used to thinking with congruences in everyday life, in a sense–"quarter past the hour" can be viewed as the class "15 modulo 60" (if we accept for argument's sake that the time unit in which we measure is a minute). It also shows the ambiguity–if we don't specify the hour or if the context doesn't make it clear, it could indicate one of a whole (ideally infinite) class of possibilities.

1.10. **Quadratic reciprocity of congruences.** One of the highlights of the term will be the exploration of a remarkable structural insight into congruences for the integers which you may not appreciate yet at this stage; to give an example: divide the prime 37 by the prime 11, giving the remainder 4, a square; so 37 leaves the same remainder as a square number when dividing by the 11—we will then say "37 is a square modulo 11". Now the "quadratic reciprocity law" found (i.e. conjectured) by Euler and Legendre and finally proved by Gauss (in six very different ways!) says that one can readily say whether the reciprocal statement "11 is a square modulo

37" holds or not, without actually having to find that square if it exists. (It does: try to divide 14^2 by 37.) We will state the amazing underlying law and give a proof.

1.11. **Other keywords,** which will be explained in due course, comprise e.g. *RSA encryption, the discrete logarithm, primitive roots modulo n* or the *Riemann hypothesis*.

1.12. **Computers.** The use of computers: especially for the cryptographic parts of our course only few examples can be carried out by hand (in decent time); hence it is almost indispensable to rely on calculators (but the range in which they are useful is still rather small) or, better still, on computers. It is very instructive to use experiments, and for this reason I recommend that you familiarise yourself with one of the following standard packages (in exams, only specific calculators will be allowed, though)

- GP-PARI (free, slim, powerful, focussed on NT);
- Maple (cheap licenses via University, big, not mainly for NT; at times somewhat unintuitive; more powerful for symbolic calculations);
- Mathematica (not so cheap student licenses (∼£100), big, multipurpose; similar ball park as Maple, great graphics routines);
- SAGE (free, huge, very powerful, strong focus on NT; versatile, unifies [i.e., it serves as a shell for other packages like the above, provided license for those is valid]).

[If there is sufficient interest, one lecture may be devoted to give an impression of how to use GP-PARI (in our context).]

2. Lecture 2 (7.10.11)

We recall a number of basic properties of the integers and the rational numbers and introduce divisibility as well as (greatest) common divisors.

2.1. **Basic properties of $\mathbb{Z}$ and $\mathbb{Q}$.** We have the following laws, according to which we are allowed to manipulate the integers and rational numbers.

(1) $(x+y)+z = x+(y+z)$ (*associativity of addition*);
(2) $xy = y+x$ (*commutativity of addition*);
(3) the equation $a+x=b$ has a unique solution x (in $\mathbb{Z}$, if a, $b \in \mathbb{Z}$, and in $\mathbb{Q}$, if a, $b \in \mathbb{Q}$);
(4) $0+x=x$ (*existence of a neutral element*);

(1') $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ (*associativity of multiplication*);
(2') $x\,y = y\,x$ (*commutativity of multiplication*);
(3') the equation $a\cdot x=b$ has a unique solution x in $\mathbb{Q}$, provided $a\neq 0$;
(4') $1\cdot x = x$ (*existence of a neutral element*);

(5) $x(y+z) = xy+xz$ (*distributive law*).

The unique solution to $a+x=b$ is written $x=b-a$.
The unique solution to $a\cdot x=b$ is written $x=\frac{b}{a}$.
(We mostly will drop the $\cdot$ sign, as usual.)

We also have a further structure on $\mathbb{Q}$ (and which is induced on $\mathbb{Z}$, viewed as a subset of $\mathbb{Q}$): an *order relation*. One can introduce it as follows:

Any rational number a is *non-negative* ($a\geq 0$) or *non-positive* ($a\leq 0$). Only 0 is both non-negative and non-positive. A number is *positive* (resp. *negative*) if it is non-negative and non-zero (resp. non-positive and non-zero). From this we can deduce the order relation between any two rationals: $b\geq a$ (or equivalently $a\leq b$) has the meaning $b-a\geq 0$, and $b>a$ (or equivalently $a<b$) has the meaning $b-a\geq 0$, $b\neq a$.

Also, we can characterise positive numbers (using the above only, positive and negative would still play symmetric roles) by demanding that if $x>0$ and $y>0$ then also $x+y>0$ and $x\,y>0$ (the corresponding statement if we replace $>$ everywhere by $<$ then cannot also hold).

2.2. **Divisibility.** If a, b, x are integers such that $ax=b$, then we say a *divides* b or "b *is a multiple of* a, and denote it by $a\mid b$. In the opposite case we write $a\nmid b$ (a does *not* divide b).

Note that $a\mid 0$ for any $a\neq 0$ (simply choose $x=0$ above).

Examples. $-5\mid 30$, $\quad 17\mid 323$, $\quad 1\mid$ any, $\quad 13\mid 13$ $\quad$ but $\quad 13\nmid 17$.

Proposition. For any integers a, b, c with a, b non-zero, we have

(1) $a\mid b \;\Rightarrow\; a\mid b\,c$;
(2) $(a\mid b \text{ and } b\mid c) \;\Rightarrow\; a\mid c$;
(3) $(a\mid b \text{ and } a\mid c) \;\Rightarrow\; a\mid b\,x+c\,y$ for any $x,y\in\mathbb{Z}$;
(4) $(a\mid b \text{ and } b\mid a) \;\Rightarrow\; a=\pm b$;
(5) $(a\mid b,\ a>0,\ b>0) \;\Rightarrow\; a\leq b$;
(6) If $m\neq 0$, then $(a\mid b \;\Leftrightarrow\; ma\mid mb)$.

Note that in (3) it is important that a is on the *left*: ($a \mid c$ and $b \mid c$) does **not** imply $(ax + by) \mid c$.

Now we introduce *common divisors*.

Definition: Let a, b be integers, not both equal to zero. A *common divisor* or a and b is any positive integer d which divides both a and b.

The *greatest common divisor* of a and b is the largest integer g with this property, i.e.,

$$g = \gcd(a, b) = \max\{d \in \mathbb{Z} \;\big|\; d \mid a \text{ and } d \mid b\}\,.$$

The integers a and b are called *coprime* or *relatively prime* if $\gcd(a, b) = 1$.

Convention: For $a = b = 0$, we put $\gcd(0, 0) := 0$.

Examples: (i) $\gcd(7, 11) = 1$.
(ii) $\gcd(-15, 25) = +5$.
(iii) $\gcd(17, 17) = 17$.
(iv) $\gcd(42, 66) = 6$.

A few obvious observations:

Remark:
(i) $\gcd(a, b) = \gcd(b, a)$;
(ii) $\gcd(a, 0) = a$.

We prepare for the Euclidean algorithm below which computes the gcd:

Lemma: For any integers a, b and q, we have

$$\gcd(a, b) = \gcd(a, b - a) = \gcd(a, b - 2a) = \cdots = \gcd(a, b - qa)\,.$$

3. Problems Class 1 (11.10.11) ["Hybrid lecture/problems class", introducing a few new notions]

3.1. **Mathematical induction and divisibility.** We recall the principle of mathematical induction, give an alternative formulation (the principle of the least element), and combine it with the notion of divisibility.

The principle of mathematical induction.
If a statement, say $P(x)$, about a positive integer x is true for $x = 1$ and its truth for all $x < n$ implies its truth for $x = n$, then it is true for all $x \geq 1$.

This principle turns out to be equivalent to the following

The principle of the least element.
Any subset of the positive integers has a smallest element.

Idea of Proof (of the second principle implying the first): We assume:
$P(x)$ is true for $x = 1$ and its truth for all $x < n$ implies its truth for $x = n$ ($*$).

Put

$$F = \{\text{all } x \geq 1 \text{ such that the statement is } \textbf{not} \text{ true for } x\}\,.$$

Then we need to show that F is necessarily empty (and hence $P(x)$ is true for all x).
We argue by contradiction: if (the subset of the positive integers) F is non-empty, then by the principle of the least element it has a smallest element, say $n \in F$. Then $P(x)$ must hold for all $x < n$ by the minimality of n. But then by assumption

$(*)$ it must also hold for n. Contradiction (as $n \in F$ means that $P(n)$ does *not* hold).

There is yet another equivalent (and probably the most familiar) way to phrase this principle, where "the statement $P(x)$ is true for $x = 1$ and its truth for $x = n - 1$ only (rather than for all $x < n$) implies the statement for $x = n$" allows to conclude that it holds for *all* $x \geq 1$.

Problem sheet 1, Q.2a) With the notation above, we put the statement $P(n)$ as follows:

$$8 \mid 5^{2n} + 7\,.$$

We first check it for $n = 1$ (the beginning of the induction): $5^2 + 7 = 32 = 4 \cdot 8$, so indeed $8 \mid 32$.
Now suppose the statement is true for n, i.e. $8 \mid 5^{2n} + 7$.
Then we need to show that $8 \mid 5^{2(n+1)} + 7$.

For this we use the above proposition, part (3):

$$(a \mid b \text{ and } a \mid c) \;\Rightarrow\; a \mid b + c$$

with $a = 8$, $b = 5^{2n} + 7$ (as we assume $P(n)$, we have $a \mid b$ here) and $c = 5^{2n+2} + 7 - (5^{2n} + 7)$.
We need to show $a \mid c$, since then we also get $a \mid b + c = 5^{2n+2} + 7$, i.e. $P(n + 1)$, and we are done.
But

$$c = 5^{2n+2} + 7 - (5^{2n} + 7) = 5^{2n}(5^2 - 1) = (5^{2n} \cdot 3) \cdot 8\,,$$

which indeed implies $a \mid c$ (as $a = 8$). □

3.2. **Division with remainder.** We use the following well-known computational tool.

Proposition (Division with remainder). If a, b are positive integers, then there exist unique integers q (the "quotient") and r (the "remainder") such that

$$a = q \cdot b + r \quad \text{and} \quad 0 \leq r < b\,.$$

Proof: 1) The *existence* is guaranteed using the principle of the least element, which we apply to the following subset

$$S^+ = \{a + bk \mid k \in \mathbb{Z} \text{ and } a + bk \geq 0\}$$

of the set $S = \{a + bk \mid k \in \mathbb{Z}\}$.
Clearly, S^+ is non-empty ($k = 0$, say) and contains only non-negative integers. By the said principle it has a smallest element, say $r(\geq 0)$. Then $r = a + bk$ for some $k \in \mathbb{Z}$.

Also $r - b = a + b(k - 1)$ ⟦use the distributive law⟧ lies in S, but cannot lie in S^+, as $r - b < r$ and r was minimal in S^+. So we can conclude that $r - b < 0$ and so $r < b$.

2) The *uniqueness* of the pair (q, r) with the above property can be seen as follows. Suppose we had two such pairs (q, r) and (q', r'). ⟦Then we want to show that they actually agree.⟧

Then we have $a = qb + r = q'b + r'$ with $0 \le r, r' < b$.
But we cannot have $q > q'$, as this would entail $r' = \underbrace{(q - q')}_{\ge 1} b + \underbrace{r}_{\ge 0} \ge b$, which is not true. As the roles of q and q' are symmetric, we cannot have $q' < q$, either. So we conclude indeed $q = q'$, and then $r' = a - q'b = a - qb = r$. □

Lemma: For any integers a, b and q, we have

$$\gcd(a, b) = \gcd(a, b - a) = \gcd(a, b - 2a) = \cdots = \gcd(a, b - qa)\,.$$

Proof: We show the first equality, the remaining ones then follow by successive application of the first. Note that it is enough to show that the set of common divisors of a and b agrees with the set of common divisors of a and $b - a$, as then necessarily also their largest elements agree.

So suppose d is any common divisor of both a and b. Then d also divides $b - a$ and hence is a common divisor of a and $b - a$.

Conversely, any common divisor d' of a and $b - a$ also divides their sum $(= b)$ and hence is a common divisor of both a and b. □

3.3. **The Euclidean Algorithm.** We illustrate this algorithm using the following example:

Compute $\gcd(345, 92)$. Using the above Lemma, we could do this as follows:

$$\begin{aligned}
\gcd(345, 92) &\overset{\text{swap}}{=} \gcd(92, 345) \overset{\text{Lemma}}{=} \gcd(92, \underbrace{345 - 3 \cdot 92}_{=69}) \\
&\overset{\text{swap}}{=} \gcd(69, 92) \overset{\text{Lemma}}{=} \gcd(69, \underbrace{92 - 69}_{=23}) \\
&\overset{\text{swap}}{=} \gcd(23, 69) \overset{\text{Lemma}}{=} \gcd(23, \underbrace{69 - 3 \cdot 23}_{=0})
\end{aligned}$$

and we know that the latter one is equal to 23.

How did we choose those multiples ($= 3$, $= 1$, $= 3$, respectively)? We wanted to make sure that the difference is both non-negative and smaller than the respective second argument in the gcd.

But note that we could instead choose a possibly different multiple: had we chosen $= 4$ in the first calculation, we would have obtained $\gcd(92, -23)$ which then would have led faster to the result. This corresponds to choosing, for integers a and $b \neq 0$, the "closest integer" to the quotient a/b. We will treat this variant in Q.4 of Problem Sheet 2.

The following scheme captures the calculations:

$$\begin{aligned}
345 &= 3 \cdot 92 + 69\,, && (q = 3,\ r = 69)\,, && \gcd(345, 92) = \\
92 &= 1 \cdot 69 + 23\,, && (q = 1,\ r = 23)\,, && \gcd(92, 69) = \\
69 &= 3 \cdot 23 + 0\,, && (q = 3,\ r = 0)\,, && \gcd(69, 23) = \gcd(23, 0) = 23
\end{aligned}$$

Once we have found a remainder $r = 0$, we are done: the gcd is then the remainder from the previous step (here $= 23$).

Bonus (from the algorithm): We can now backtrace and find our gcd (i.e., 23) as an integer linear combination of the input data (i.e., 345 and 92):

$$23 = x \cdot 345 + y \cdot 92\,.$$

How so? Start with the penultimate row in the above scheme and rearrange it a bit:

$$23 = 93 - 1 \cdot 69\,.$$

Then use the row above that one to rewrite the right hand term (i.e. 69):

$$69 = 345 - 3 \cdot 92\,.$$

Now plugging this latter equation into the former, we find

$$\begin{aligned} 23 &= 92 - (345 - 3 \cdot 92) \\ &= (3+1) \cdot 92 - 345\,. \end{aligned}$$

4. Lecture 3 (13.10.11)

The above example illustrates the following important statement:

Theorem: (Euclidean Algorithm) Let a, b be integers, then use the division algorithm to successively find q_i (quotients) and r_i (remainders) in $\mathbb{Z}$ with $0 \leq r_i < r_{i-1}$, $(i = 0, 1, 2, \dots)$, where we put $r_0 := b$, and such that

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n + r_{n+1} \end{aligned}$$

until some remainder, say r_{n+1}, equals zero, then stop. In this case, r_n is the gcd of a and b.

Proof: By the lemma above, we have

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, r_{n+1}) = r_n\,.$$

Moreover, the algorithm stops after finitely many steps: we have $r_0 > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$ (i.e. the remainders get strictly smaller at each step) and there are only finitely many integers between 0 and r_0. □

: Show that, for the remainders $r_0 > r_1 > \cdots > r_n > 0$ in the Euclidean algorithm one has

$$r_{j+2} < \frac{1}{2}\, r_j \qquad (0 \leq j < n)\,.$$

Corollary: For any a, $b \in \mathbb{Z}$, we can find integers x, y such that

$$\gcd(a, b) = ax + by\,.$$

Proof: Use induction on the *index* j of the remainders r_j, as they appear in the Theorem above:

1. The statement holds for $j = 0$ and $j = 1$, since $r_0 = b = ax_0 + by_0$ ($x_0 = 0$, $y_0 = 1$) and $r_1 = a - q_1 b = ax_1 + by_1$ ($x_1 = 1$, $y_1 = -q_1$).

2. Suppose the statement holds for all non-negative $k \leq j$, i.e.

$$r_k = ax_k + by_k \qquad \text{for some } x_k, y_k \in \mathbb{Z}\,.$$

Then we prove it also for $j+1$:

$$\begin{aligned} r_{j+1} &= r_{j-1} - q_{j+1} r_j \\ &= (ax_{j-1} + by_{j-1}) - q_{j+1}(ax_j + by_j) \\ &= a(x_{j-1} - q_{j+1}x_j) \;+\; b(y_{j-1} - q_{j+1}y_j) \end{aligned}$$

and we can put $x_{j+1} = x_{j-1} - q_{j+1}x_j$ and $y_{j+1} = y_{j-1} - q_{j+1}y_j$. □

Explicitly, it may be best to start from the penultimate line $r_n = r_{n-2} - q_n r_{n-1}$ (where $r_{n+1} = 0$), then substitute r_{n-1} using a similarly rearranged third-to-last line, etc.

For a formal description (for implementation on a computer) see Stein's book, Algorithm 1.1.13.

Primes: There are distinguished integers with the least possible number of divisors.

Definition: A positive integer $n > 1$ is **prime** if its only positive divisors are 1 and n itself. Otherwise n is called **composite**.

⟦Note that the integers 0 and 1 are neither prime nor composite.⟧

List of the first primes:

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

List of the first composites:

$$4, 6, 8, 9, 10, 12, \ldots$$

An important property of the primes (which will be the *defining* property of primes in more general contexts than $\mathbb{Z}$) is the following:

Theorem (Euclid): Let p be a prime and a, $b \in \mathbb{Z}$. Then we have:
if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Suppose $p \mid ab$. If $p \mid a$, we are done. Hence we can assume that $p \nmid a$; but the only positive divisors of p are 1 and p, so the only (positive) *common* divisor of a and p is 1, hence also the maximum of all common divisors, i.e. the gcd of a and p.

By the Corollary to the Euclidean Algorithm we can find x, $y \in \mathbb{Z}$ such that

$$ax + py = 1\,.$$

Multiply both sides by b to get

$$abx + pby = b\,,$$

and since $p \mid ab$ and $p \mid pby$, we deduce that p must also divide the combination $abx + pby$, hence b. □

Factoring into Primes: We first notice that each number $n > 1$ can be factored into primes: we argue by induction, assuming that each positive number $< n$ (different from 1) is a product of primes, and more precisely a *finite* such product. Now either n is itself prime, in which case we are done, or n is composite, in which case there must be a way to write $n = ab$ for some integers a, b (which we can both assume to be positive) with $a < n$ and $b < n$. By induction assumption (and noting that neither a nor b equals 1), both a and b can be written as a product of primes. Hence also their product.

Empty products. We can even include 1 in the description above if we use the standard convention that an empty product equals 1.

A remark about the "empty product": we first consider the analogous situation of an "empty sum"—take a sum and break it up into two subsums:

$$\sum_{j=1}^{n} f(j) = \sum_{j=1}^{r} f(j) + \sum_{j=r+1}^{n} f(j) \qquad (r = 1, \dots, n-1)\,.$$

It is useful to write this in terms of "index(ing) sets":

$$\sum_{j\in S_n} f(j) = \sum_{j\in S_r} f(j) + \sum_{j\in S'_r} f(j) \qquad (r = 1, \dots, n-1)\,, \tag{1}$$

where $S_n = \{1, \dots, n\}$, $S_r = \{1, \dots, r\}$ and $S'_r = \{r+1, \dots, n\}$. Clearly we have $S_n = S_r \cup S'_r$ (in fact, this is a disjoint union).
Now consider the "extremal" case where we allow $r = 0$, then we want this decomposition to still hold. But then $S_r = \{\}$ is the empty set and $S'_r = S_n$, so the only sensible definition for $\sum_{j\in S_r} f(j)$ is to set it to zero, otherwise the equality would not hold in (1).

Similarly, we can argue for products: if we want to extend

$$\prod_{j\in S_n} f(j) = \prod_{j\in S_r} f(j) \cdot \prod_{j\in S'_r} f(j) \qquad (r = 1, \dots, n-1)\,, \tag{2}$$

to $r = 0$, say, then the only sensible way to define $\prod_{j\in S_r} f(j)$ is to put it $= 1$.

Perhaps it is also useful to recall the meaning of the special case a^r (put $f(j) = a$ for any j above) in the "extremal" case $r = 0$: the only way to define it compatibly with the usual arithmetic operations is to put it equal to 1. ⟦Note that, rather counterintuitively, even $0^0 = 1$.⟧

5. Lecture 4 (14.10.11)

The above decomposition into primes turns out to be unique (in a certain well-defined sense), which is the statement of the

Fundamental Theorem of Arithmetic: Every positive integer can be written as a product of primes in a unique way (up to order).

As a preparation, we give the following generalization of Euclid's theorem above:

Corollary: Let p be a prime and $a_1, \dots, a_n \in \mathbb{Z}$ for some $n \geq 1$. Then we have: if $p \mid a_1 \cdots a_n$, then p divides one of the a_i $(1 \leq i \leq n)$.

⟦Pf: Deduce from Euclid's theorem above, using induction: $p \mid a_1 a_2 \cdots a_n$ implies $p \mid a_1$ or $p \mid a_2 \cdots a_n$; in the first case we are done, otherwise we keep going... ⟧

Proof (of FTA): "Existence": We have proved above, using induction, that we can write every positive integer as a product of primes (with the special case that 1=empty product of primes).

"Uniqueness": Suppose we have two factorizations of a number n into primes, i.e.

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \,,$$

where all p_i $(1 \le i \le r)$ and all q_j $(1 \le j \le s)$ are primes. We can assume $r \le s$.

Then we will show that the primes have to match one by one.

Start with p_1: we know $p_1 \mid n$ and hence $p_1 \mid q_1 q_2 \cdots q_s$, so by the above Corollary we get $p_1 \mid q_j$ for *some* $j \in \{1, \ldots, s\}$. After reordering we can assume $j = 1$, so that $p_1 \mid q_1$. But q_1 is prime and has as its only non-trivial positive divisor itself, so necessarily $p_1 = q_1$ (both are positive). We can cancel p_1 on both sides (use Proposition, part (6), in §.2.2) and keep going: we find $p_2 \cdots p_r = q_2 \cdots q_s$ and can repeat the previous argument to show that, up to reordering, $p_2 = q_2$ and this can be cancelled, too. This procedure can be repeated until the last p_r is cancelled as well, so that we have $1 = q_{r+1} \cdots q_s$, but this means that on the RHS we must have the empty product. Therefore both factorizations above of n are identical. □

Immediate questions:

Q1: How can we check whether a number $n > 1$ is prime or composite?

Q2: Suppose n is composite, how can we find a factorization?

It turns out that Q1 is much easier than Q2; this is clear for numbers like 2001 where we see one factor (i.e. 3) easily, so $2001 = 3 \cdot 667$ is clearly composite. But it is not quite so easy to get the full prime decomposition $2001 = 3 \cdot 23 \cdot 29$.

Better still, we will find a way to detect rather quickly that a number is composite without in general having to find its prime decomposition. In particular, it is easy to cook up a product $n = pq$ of two large primes p and q that your computer will not be able to factor, even though it can check readily that n is not prime itself.

How many primes? Our first quantitative insight into the primes is again due to Euclid:

Theorem: There are infinitely many primes.

Proof (by contradiction): Suppose there are only finitely many primes $p_1, p_2, \ldots, p_r$. Then consider $N := p_1 \cdot p_2 \cdots p_r + 1$.

Now $N = q_1 \cdots q_s$ for some primes q_j $(j = 1, \ldots, s$, where $s \ge 1)$ by the FTA, and clearly $\gcd(p_i, q_j) = 1$ for any i, j, since

$$1 = p_i x + q_j y$$

for the integers $x = -p_1 \cdots p_{i-1} p_{i+1} \cdots p_r$ and $y = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s$. Therefore the list $\{p_1, \ldots, p_r\}$ cannot hold all the primes (e.g. q_1 is missing), contradicting our assumption.
Conclusion: there must be infinitely many primes. □

Note that the first few such numbers,

$$\begin{aligned} N &= 2+1\,, \\ N &= 2\cdot 3+1=7\,, \\ N &= 2\cdot 3\cdot 5+1=31\,, \\ N &= 2\cdot 3\cdot 5\cdot 7+1=211\,, \\ N &= 2\cdot 3\cdot 5\cdot 7\cdot 11+1=2311, \end{aligned}$$

are all themselves primes, so at first sight one might be tempted to hope that this behaviour perhaps persists, but already the next one in the list, $N = 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1$ factors (as $59\cdot 509$).

With a bit more work we can prove a more refined (and striking) statement about the infinity of primes of a given form. We prepare for it with the following straightforward

Remark: The product of two numbers of the form $4n+1$ is again of this form. ⟦Proof: $(4n_1+1)(4n_2+1) = 16n_1n_2+4n_1+4n_2+1 = 4(4n_1n_2+n_1+n_2)+1$.⟧

Theorem: There are infinitely many primes of the form $4n-1$.

Proof: Suppose there are only finitely many such primes, $p_1,\dots,p_r$, each p_i being of the form $4m_i-1$ for some $m_i \geq 1$.
Then we for the odd number $N := 4p_1\cdots p_r - 1$ which clearly shows $\gcd(N,p_i)=1$, but which factors into (odd) primes which cannot all be of the form $4n+1$ by virtue of the above remark, since N itself is not of this form. Hence there must be at least one prime of the form $4n-1$ dividing N ⟦all odd primes are either of the form $4n+1$ or $4n-1$⟧ and moreover it is coprime to all the p_i.

Hence, like in Euclid's proof, we see that our assumption cannot hold, and we conclude that there must be infinitely many primes of the form $4n-1$, as claimed. □

6. Lecture 5 (20.10.11)

From last time: there are different (rather similar) constructions to prove the infinity of primes. Euclid's argument is flexible: suppose the set $\mathbb{P}$ of primes (of a certain type) is finite, say $\mathbb{P} = \{p_1,\dots p_r\}$. Then we find a contradiction by constructing new primes, using FTA. A crucial identity is that there are primes q_1, $\dots q_s$ such that

$$q_1\cdots q_s = N = p_1\cdots p_r\cdot M \pm 1\,,$$

where M can be any positive integer: last time we took $N = (p_1\cdots p_r)+1$ (for showing that there are infinitely many primes) and $N = 4(p_1\cdots p_r)-1$ (to show that there are infinitely many primes of the form $4k-1$). ⟦Of course the second statement also implies the first.⟧

One important property we need is:

$$\gcd(q_1,p_j) = 1 \text{ for any } j = 1,\dots,r.$$

and this is clear, regardless of M, as the above equation writes 1 as an integer linear combination of q_1 and p_j.

So q_1 must be a prime different from the p_j, and if we can guarantee that it is itself of the type in question, then we arrive at the sought-for contradiction.

Exercise. In a similar way, one can try to prove that there are infinitely many primes of the form $6n-1$: suppose there is a finite list $p_1, \ldots, p_r$ of such primes, then consider $N = 2 \cdot 3 \cdot p_1 \cdots p_r - 1$ and use that there are
1.) few primes of the form $6n-3$ (which?) and
2.) the set of numbers of the form $6n+1$ is closed under multiplication.

Note: It is also true that there are infinitely many primes of the form $4n+1$, but this is somewhat harder to prove. At least if we assume as known the following statement (not too hard, uses properties of quadratic residue which we introduce towards end of term):

Theorem: for coprime integers a and b, with $a > b \geq 1$, any odd prime dividing $a^2 + b^2$ is of the form $4n+1$.

then we can get a Euclid-type proof: suppose there is a finite list $p_1, \ldots, p_r$ of such primes, then we form the odd number $(p_1 \cdots p_r)^2 + 4$ and use the above theorem $[\![a = p_1 \cdots p_r,\ b = 2$ are clearly coprime$]\!]$ to arrive at a contradiction.

But there is a much more general theorem known (but far beyond the scope of the course): Let us put

$$S_{a,b} = \{ak + b \mid k \in \mathbb{Z}\}\,.$$

Theorem (Dirichlet's theorem on arithmetic progressions): For coprime a and b there are infinitely many primes in $S_{a,b}$.

As examples we had seen proofs for $S_{4,-1}$, $S_{6,-1}$ (exercise), $S_{4,1}$ (conditionally) and $S_{1,0}$ (Euclid)—of course all three former ones imply the statement of the latter.

The proof of Dirichlet's Theorem is far beyond the scope of the lectures; it uses subtle methods of analytic number theory (non-vanishing of "L-series" at a very specific point; we will actually encounter a very special such L-series below).

Remark: One can even prove, using sophisticated tools from analytic number theory, that "about half the primes" are of the form $4k-1$ and "the other half" (we can disregard the only other prime 2 here) are of the form $4k+1$. More precisely, this is an asymptotic statement taking the quotient of the number of primes below a given bound with the extra property by the full number of primes below that bound.

An Euler product. A different "proof" of the infinitude of primes (with a beautiful insight, albeit with a somewhat non-rigorous method) has been given by Euler, a sketch of which is as follows:

The idea is to write, for real $s > 1$, the sum of the inverse s^{th} powers of the positive integers

$$\Sigma_s := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

and to realise that it can be written as a product over all the primes (so-called *Euler product*)

$$\begin{aligned}\Pi_s &:= \left(1+\frac{1}{2^s}+\frac{1}{2^{2s}}+\frac{1}{2^{3s}}+\frac{1}{2^{4s}}+\dots\right)\\ &\times \left(1+\frac{1}{3^s}+\frac{1}{3^{2s}}+\frac{1}{3^{3s}}+\frac{1}{3^{4s}}+\dots\right)\\ &\times \left(1+\frac{1}{5^s}+\frac{1}{5^{2s}}+\frac{1}{5^{3s}}+\frac{1}{5^{4s}}+\dots\right)\\ &\vdots\end{aligned}$$

Let us again suppose, for a contradiction, that there are only finitely many primes $p_1 = 2, p_2 = 3, p_3 = 5, \dots, p_r$. The FTA guarantees that each term (i.e. n^{-s}) in the sum occurs *precisely once* when multiplying out this Euler product, using the *unique* prime factorization: each n has a prime factorization $n = 2^{a_1}3^{a_2}5^{a_3}\cdots p_r^{a_r}$ with $a_1 \geq 0, \dots, a_r \geq 0$, and hence n^{-s} in the sum corresponds to the corresponding product of terms $\frac{1}{2^{a_1 s}}, \frac{1}{3^{a_2 s}}, \dots, \frac{1}{p_r^{a_r s}}$.

Note that the respective lines in that product can now be rewritten using the geometric series expression

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$

as $\frac{1}{1-2^{-s}}$, $\frac{1}{1-3^{-s}}$, $\frac{1}{1-5^{-s}}$ etc.

Now take the limit when $s \to 1$; then $\Pi_1 = \frac{1}{1-2^{-1}} \cdot \frac{1}{1-3^{-1}} \cdots \frac{1}{1-p_r^{-1}}$ is a rational number, but we know from Analysis, say, that $\Sigma_1 = \sum_{n\geq 1} 1/n$ (the so-called *harmonic sum*) is divergent ⟦e.g. group the terms for $n \geq 2$ into packages of 1, 2, 4, 8, etc. terms $\frac{1}{2}$, $\frac{1}{3}+\frac{1}{4} \geq 2\cdot\frac{1}{4}$, $\frac{1}{5}+\dots+\frac{1}{8} \geq 4\cdot\frac{1}{8}$, etc, each of these infinitely many packages being $\geq \frac{1}{2}\dots$⟧.

This contradiction shows that there cannot be only finitely many primes.

The above argument can in fact be made rigorous (e.g. Scharlau/Opolka: "From Fermat to Minkowski").

7. Lecture 6 (21.10.11)

How to test for primeness?

If we want to test naively whether a number n is prime, all we need to check is whether any of the primes less than n divides it: this is clear since if n is composite, there must be a number m strictly between 1 and n dividing it, and this number is a product of primes by the FTA, hence each of those primes (which are $\leq m$ by one of our earlier propositions) divides n.

But we can do better: if n is composite, it can be written as ab for some positive integers $1 < a, b < n$, we can assume $a \leq b$, and then a must be $\leq \sqrt{n}$ ⟦otherwise $n = \sqrt{n}\sqrt{n} < a\,b$, a contradiction.⟧

Hence all we need to check are the primes less than or equal to $\sqrt{n}$. We have proved:

Lemma: If a positive integer n is not divisible by any prime $\leq \sqrt{n}$, it is itself prime.

This is a very clumsy way to check for primeness, at least for larger numbers. We will encounter much quicker ways ("primality tests") to establish that a given number is prime.

Finding or constructing primes?
How to "construct" primes? This is a rather intractable problem. For example, there is no function known which produces infinitely many (different) primes, and primes only.

From Euclid's theorem we deduce that there is no "largest prime"... But it is a kind of sports to *find* large primes. Typically they are of a very special form: most likely contenders for such record primes are so-called "Mersenne primes" of the form $2^n - 1$ (if a prime is of this form, then n can be shown to be necessarily prime, but not all numbers of the form $2^n - 1$ with n prime are themselves primes, cf. Sheet 3, Q5b).

The largest **currently known** prime is the 12,978,189 digit Mersenne prime $2^{43112609} - 1$ found in August 2008 (see e.g. the website by Chris Caldwell, Univ. of Tennessee, `http://primes.utm.edu/notes/by_year.html`).

Famous open problems: There are still many unknown ancient questions on the primes, e.g.

- Are there infinitely many primes of the form $n^2 + 1$?
- Are there infinitely many "prime twins", i.e. pairs $(p, p + 2)$ such that both p and $p + 2$ are prime?
- (Goldbach problem) Is any even number a *sum of two* primes?

Vinogradov (1937) showed that each *sufficiently large* odd integer is the sum of 3 primes.
Also, Chen (1966) proved a statement that comes rather close to Goldbach's problem: every sufficiently large even number is a sum of a prime and an "almost-prime" (an almost-prime is a number > 1 which has at most two prime factors).

Arithmetic progressions of primes: Instead of looking for primes in arithmetic progressions, we can reverse the roles and ask whether we can find long sequences of "equidistant" primes: e.g. we can see that the elements in the 5-term sequence

$$5, 11, 17, 23, 29$$

are all prime and the difference between successive pairs is the same ($= 6$).

Record progressions:

- length 6: $7 + 30 \cdot n$ (found in 1909 by G. Lemaire)
- length 10: $199 + 210 \cdot n$ (found 10^2 years ago, in 1910, by Edward B. Escott):
- The first one of length 11 needed to wait until 1999 (using an 8-digit number in place of 199)...

For more detail, visit the homepage of Jens Kruse Andersen;
`http://users.cybercity.dk/~dsl522332/math/aprecords.htm`

Longest known arithmetic progression: In 2010 Benoît Perichon (and PrimeGrid) found the first known arithmetic progression of length 26:

$$43142746595714191 + 23681770 \cdot 23\# \cdot n\,, \text{ for } n = 0, \ldots, 25, \text{ are all prime.}$$

Here $k\#$ denotes the product of all primes below or equal to k.

The theoretical result is much better here (outstanding recent progress, earned T.Tao a Fields medal), albeit it does not give a method to find any specific example:

Theorem (Tao-Green, 2004): The primes admit arbitrarily long progressions.

The Prime Number Theorem (a rather impressionist subsection)
Having established the infinity of primes (and e.g. of primes of the form $4n-1$), we can ask further questions:

How are the primes distributed? Are there more than, say, the number of integer squares? Suppose we found a prime p, can you find the next prime within reasonable proximity?

Given $N > 1$, is there a prime in the interval $[N, 2N]$? Assuming the truth of this statement was known as "**Bertrand's postulate (1845)**", and the statement was later proved indeed by Chebyshev (1845), giving rise to the following "cursory rhyme" (due to N.Fine in 1999), see the Springer book *Prime numbers* by Crandall and Pomerance, p.55):

Old Che*byshev* said *it,*
we'll say *it a*gain:
there's al*ways a* prime
between N and 2*N*.

There is recent work on analogous results, both proved in an elementary fashion (improving on the above):
1) for $N > 1$, there is always a prime between $2N$ and $3N$ (El Bachraoui, 2006);
2) for $N > 2$, there is always a prime between $3N$ and $4N$ (Andy Loo, 2011).

8. Lecture 7 (27.10.11)

What is a good measure to state something meaningful about "how many"?

The Prime Counting Function $\pi(x)$ is defined as

$$\pi(x) := \text{ number of primes below or equal to } x\,.$$

We can get a first impression of how large it becomes, say, if we compute it for $x \,:\, [10, 10^2, \ldots, 10^{10}]$:
$\pi(x) \,:\, [4, 25, 168, 1229, 9592, 78498, 664579, 5761455, 50847534, 455052512]$
If we consider the quotient $x/\pi(x)$ for these, we find, respectively,

$$[2.5, 4.0, 6.0, 8.1, 10.4, 12.7, 15.0, 17.4, 19.7, 22.0]$$

whose differences "stabilise" and tend to go to 2.3 which is roughly $\log(10)$ where log denotes the natural logarithm (to base e).

Therefore we see (for $j = 1, \ldots, 10$) that we might expect that for any $j > 0$ we have

$$\frac{10^j}{\pi(10^j)} - \frac{10^{j-1}}{\pi(10^{j-1})} \approx \log(10)\,,$$

where $\approx$ denotes "approximately" and by "telescoping" we find

$$\frac{10^j}{\pi(10^j)} - \underbrace{\frac{10^1}{\pi(10^1)}}_{=2.5} = \sum_{k=2}^{j} \Big(\frac{10^k}{\pi(10^k)} - \frac{10^{k-1}}{\pi(10^{k-1})} \Big) \approx (j-1)\log(10)\,.$$

Hence by interpolation we are led to guess the following, already conjectured by Legendre and Gauss (late 18th century), where for two functions A and B we now denote by $A(j) \sim B(j)$ that A and B are asymptotically equivalent, i.e. $\lim_{j\to\infty} A(j)/B(j) = 1$:

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log(x)}\,.$$

Stated slightly differently, we have

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1\,.$$

This famous theorem was conjectured by Legendre and Gauss (around 1800), on the evidence of lots of calculations by hand, and was proved (in a non-elementary way) independently by Hadamard and by de la Vallée-Poussin in 1896). There is a link to a short *elementary* proof by Zagier (adapting an idea of Newman) on the course page.

The original proofs of the Prime Number Theorem used the function $\zeta(s) := \sum_{n\geq 1} n^{-s}$ from Lecture 5, called the **Riemann zeta function**, an extremely important function in Number Theory.
Amazingly, that proof boils down to showing that $\zeta(s)$ never vanishes on the line $\Re(s) = 1$ (i.e. $\zeta(1+it) \neq 0$ for $t \in \mathbb{R}$, $i^2 = -1$).

There is in fact a much stronger result expected: first of all, this function can be "analytically continued" to a function on the whole complex plane (except for a pole at the point $s = 1$), and it makes even sense to talk about $\zeta(s)$ at negative integers.

Surprise: One has

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}\,,$$

[not a trivial result at all!] and using a special symmetry ("functional equation") relating $\zeta(s)$ to $\zeta(1-s)$, one obtains

$$\zeta(-1) = -\frac{1}{12}\,.$$

As a series, this would imply the crazy identity

$$\zeta(-1) \;=\; 1+2+3+4+\ldots \;=\; -\frac{1}{12}\,. \qquad (**)$$

⟦Here is an "Euler type argument" for this equailty (not rigorous, but quite instructive!): recall the geometric series in the form

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \ldots$$

from which we get, by differentiation (term-wise on the right)

$$-\frac{1}{(1+x)^2} = \frac{d}{dx}\Big(\frac{1}{1+x}\Big) = -1 + 2x - 3x^2 + - \ldots$$

Now substitute $x = 1$ to get

$$\frac{1}{4} = \frac{1}{(1+1)^2} = 1 - 2 + 3 - + \cdots =: R$$

and use further that

$$\begin{array}{rcrrrr} S & = & 1+2 & +3+4 & +5+6 & +\ldots \\ -4S & = & -4 & -8 & -12 & -\ldots \\ \hline -3S & = & 1-2 & +3-4 & +5-6 & +-\ldots \end{array}$$

to finally deduce

$$\frac{1}{4} = R = -3S\,,$$

which is the claim $(**)$ above.⟧

The Riemann zeta function turns out to have "trivial" zeros at all the negative *even* integers (i.e. $\zeta(-2n) = 0$ for $n \geq 1$, $n \in \mathbb{Z}$).

More important are the "non-trivial" zeros which are expected to be all on a single line: this turns out to be one of the most important (and intractable) problems in mathematics, the so-called

Riemann Hypothesis: The non-trivial zeros of $\zeta(s)$ all lie on the line $\Re(s) = \frac{1}{2}$.

The truth of this hypothesis (and hardly anyone doubts it) would have far-reaching consequences for many counting problems in NT (in a far from obvious manner), and moreover it has $\$10^6$ prize money on it.

9. Lecture 8 (28.10.11)

Congruences. Our next topic are *congruences*. This notion captures very conveniently the properties of divisibility that we have encountered, and it suggests a calculus based on those.

Definition: For integers a, b and $n \geq 1$, we define

$$a \equiv b \pmod{n}$$

(in words: "*a is congruent to b modulo n*"), whenever $n \mid a - b$.
Sometimes n is called the *modulus*.

In other words: a is congruent to b if both numbers leave *the same remainder* when dividing by n.

Simple properties:

(i) In particular, $a \equiv a$ modulo any $n \geq 1$.

(ii) Also, if a is congruent to b, then clearly b is congruent to a ("leaving the same remainder" does not prefer any of the two numbers involved).

(iii) Furthermore, if a is congruent to b modulo n, and also b is congruent to c modulo n (for some $c \in \mathbb{Z}$), then a is also congruent to c modulo n ⟦all three leave the same remainder modulo n; another way to see this is to use that $rn = a - b$ and $sn = b - c$ (for some r, $s \in \mathbb{Z}$) implies $(r + s)n = a - c$ ⟧.

Properties (i)–(iii) above show:

Proposition: Congruence modulo a fixed modulus n defines an equivalence relation.

Therefore the integers are partitioned into n different equivalence classes modulo n (one for each possible remainder $0 \leq r < n$). The equivalence *classes* with respect to this relation are the objects with which we will compute!

Notation: The equivalence class of an integer a modulo a positive integer n is denoted by $[a]_n$ or, provided the context is clear, simply by $[a]$.
Note that the elements in $[a]$ (we fix n here) are precisely the ones of the form $a + kn$, where k runs through the integers.

For example, for $n = 5$ we have the following classes (one each per column in the table below):

$$\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \vdots \\ -5 & -4 & -3 & -2 & -1 \\ 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

Example: the equivalence class $[17] = [17]_5$ of 17 in this partition of $\mathbb{Z}$ is given by the middle column $[17] = \{\dots, -8, -3, 2, 7, 12, 17, \dots\}$.

Arithmetic modulo n. For *fixed modulus* n we want to add and subtract and even multiply such classes. How can we compute with "infinitely many objects" at the same time? The answer is: pick any number in the respective classes and perform the usual arithmetic for the so picked integers, and then define *the class modulo n of the result* as the outcome; in formulas: if we choose integers a and b, then we define for their classes modulo n the following two binary operations:

$$[a] \boxplus [b] := [a + b]\,, \qquad [a] \boxdot [b] := [a \cdot b]\,.$$

Why does this work, i.e. why is this well-defined? This is a direct consequence of the properties of divisibility by n: suppose we choose any element in each of the two classes, e.g. $a' \in [a]$, $b' \in [b]$, then we can write $a' = a + kn$ and $b' = b + \ell n$ for some integers k, ℓ, and we have $a' + b' = a + b + (k + \ell)n$ and $a'b' = ab + (kb' + \ell a' + k\ell n)n$ and hence

$$\begin{aligned} a + b &\equiv a' + b' \pmod{n}\,, \\ a \cdot b &\equiv a' \cdot b' \pmod{n}\,. \end{aligned}$$

What should we take as "negative $[a]$"?

Notation: The set of equivalence classes forms a *ring* (cf. Algebra), denoted $\mathbb{Z}/n\mathbb{Z}$.

What is more, we can sometimes (not always) divide: as a preparation for this, we have

Lemma: If $n \mid ab$ and $\gcd(n, a) = 1$ then $n \mid b$.
⟦Proof: as for Euclid's Thm: write $1 = xa + yn$ and multiply by b; n divides RHS, hence LHS.⟧

Proposition: Let a, b, $c \in \mathbb{Z}$ and $n \geq 1$ such that $\gcd(c, n) = 1$. Then if

$$ac \equiv bc \pmod{n}\,,$$

then $a \equiv b \pmod{n}$.

Proof: From $n \mid ac - bc = c(a - b)$ and the above lemma we get $n \mid a - b$. □

As an application, we can justify the "casting out nines" method, which claims that in order to check that a number is divisible by 9, we can just as well check that the sum of its digits is. In mathematical terms:

Proposition: (i) A number n is divisible by 9 if and only if the sum of its digits is divisible by 9.
(ii) A number n is divisible by 11 if and only if the *alternating* sum of its digits is divisible by 11.

Proof: We will prove something slightly stronger. Write n in its decimal expansion, i.e.,

$$n = a_0 + 10a_1 + 100a_2 + \cdots + a_k 10^k, \quad \text{for some } k \geq 0 \text{ and } 0 \leq a_j \leq 9 \quad (j = 0, \ldots, k).$$

(i) Then note that

$$\begin{aligned} 10 &\equiv 1 \pmod 9, \\ \text{hence} \quad 10 \cdot 10 &\equiv 1 \cdot 1 \pmod 9, \\ \text{in fact} \quad 10^j &\equiv 1 \pmod 9, \qquad \text{for any } j \geq 1. \end{aligned}$$

So $n = a_0 + 10a_1 + 100a_2 + \cdots + a_k 10^k \equiv a_0 + a_1 + \cdots + a_k \pmod 9$, from which the claim follows.

(ii) Note further that $10 \equiv -1 \pmod{11}$, hence $10^2 \equiv +1 \pmod{11}$ and inductively $10^j \equiv (-1)^j \pmod{11}$. So $n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$, proving the second claim. □

Instead of working with those (infinite) equivalence classes, it is more convenient to work with representatives.

Definition: A **complete set of residues modulo** n is a subset $R \subset \mathbb{Z}$ of size n whose remainders modulo n are all different.

There is a natural choice of such a set by simply choosing the possible remainders modulo n: $R = \{0, 1, 2, \ldots, n-1\}$ constitutes a complete set of residues modulo n. A far less natural choice for, say, $n = 7$ would be

$$R = \{-35, 15, 23, -4, 4, -9, 97\}.$$

You can use PARI to check the above (using `%` as the "modulo operator", e.g. `15%7` should output `1`, and conveniently we can even apply this to a whole vector in one go):
`[-35,15,24,-4,4,-9,97]%7` should output `[0,1,2,3,4,5,6]`.
Similarly, in MAPLE we use `[-35,15,23,-4,4,-9,97] mod 7;` instead.

A crucial observation is now that we can sometimes pass from one such complete set of residues to another (for the same modulus n):

Lemma: Let R be a complete set of residues modulo n and a any integer which is coprime to n.
Then $aR := \{ax \mid x \in R\}$ is *also* a complete set of residues modulo n.

Proof: Why should all the elements in R be in different classes? Suppose we get $ax \equiv ax' \pmod n$ then, since $\gcd(a, n) = 1$, we can apply the cancellation lemma above to get $x \equiv x' \pmod n$. This shows that aR contains elements from at least n different classes; but there are only n such. Hence aR is indeed a complete set of residues modulo n. □

We are aiming for a famous result: Fermat's Little Theorem, which claims that, for p prime and $\gcd(a, p) = 1$, we have

$$a^{p-1} \equiv 1 \pmod p.$$

There is even a generalization of this, which goes by the name of "Euler-Fermat", where the prime p is replaced by any $n > 1$. Since its proof proceeds along the same lines, we try to cover the more general case instead.

10. Lecture 9 (3.11.11)

As a preparation for the Euler–Fermat Theorem, we look at linear congruences (essentially the asme as linear equations, except $=$ is replaced by $\equiv$ with respect to some modulus) and Euler's φ-function.

Definition: A *linear congruence* is an equation of the form

$$ax \equiv b \pmod{n},$$

where a, b, and n are given integers ($n > 0$).

Proposition: For a, b, $n \in \mathbb{Z}$ with $\gcd(a, n) = 1$ the linear congruence $ax \equiv b \pmod{n}$ has a solution. Moreover, the solution is unique up to adding multiples of n.

Proof: Let R be a complete set of residues modulo n (e.g., choose the "natural" one mentioned above). There is precisely one element in R which is congruent to b modulo n. By the above lemma, there is also one element, in fact a unique one, in aR with this property—here we use that $\gcd(a, n) = 1$. But this element has the form ax (for some $x \in R$), and so we get $ax \equiv b \pmod{n}$. □

Example: Solve the linear congruence

$$3x \equiv 2 \pmod{11}$$

as follows: take the natural choice $R = \{0, 1, 2, \ldots, 10\}$ from which we get that $3R = \{0, 3, 6, 9, 12(\equiv 1), 15(\equiv 4), 18(\equiv 7), 21(\equiv 10), 24(\equiv 2), 27(\equiv 5), 30(\equiv 8)\}$. The unique number in $3R$ which is congruent to $2 \pmod{11}$ is 24 which corresponds to $x = 8$ in R.

If the modulus is a bit larger, it may be wise not to simply try out all numbers, e.g. for

$$5x \equiv 17 \pmod{199}$$

it may be useful to first find an x' such that $5x' \equiv 1 \pmod{199}$ (which is considerably easier in this case, since $1 \equiv 200 \pmod{199}$) and then multiply $x'(= 40)$ by 17 to get $x(= 680)$, which then can (but need not) be reduced mod 199.

Proposition: A linear congruence $ax \equiv b \pmod{n}$ is solvable if and only if $\gcd(a, n) \mid b$ (without proof, cf. e.g. Niven–Zuckerman, Thm 2.17 (p.62)). □

Before stating the central theorems, we need one more notion:

Definition: *Euler's totient function* or *Euler's φ-function* is defined as

$$\varphi(n) = \#\{r \in \mathbb{Z} \mid 0 < r < n \text{ and } \gcd(r, n) = 1\},$$

i.e., as the number of positive integers below n which are coprime to it.

Euler-Fermat Theorem. For $n > 0$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$ we have

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof: We consider

$$P = \{r \in \mathbb{Z} \mid 0 < r < n \text{ and } \gcd(r, n) = 1\},$$

which has the property that it comprises all those residues modulo n which are *coprime to* n. Moreover, we use that aR also has that property by a previous lemma, as $\gcd(a,n)=1$. Therefore the *product* over all elements in P leaves the same remainder modulo n as the product over the elements in aP, i.e.

$$\prod_{r\in P}(ar)\equiv\prod_{r\in P}r\,.$$

Now cancelling the $r\in P$ one by one (as we can by cancellation lemma) we get

$$\prod_{r\in P}a\equiv 1\,,$$

but a is independent of the running index r, so the LHS equals $a^{\#\{r|r\in P\}}=a^{\varphi(n)}$. □

11. Lecture 10 (4.11.11)

We had seen the Euler-Fermat Theorem, and as a simple consequence we get:

Corollary (Fermat's Little Theorem):
For p prime and $a\in\mathbb{Z}$ such that $\gcd(a,p)=1$ we have

$$a^{p-1}\equiv 1 \pmod p\,.$$

Proof: We have $\varphi(p)=p-1$, since each r such that $0<r<p$ is coprime to p. □

Example: Suppose we want to know what weekday we will have a million days from today. (How long is that in years, roughly? $365\cdot 3$ is a bit larger than 1000, so it would be in less than 3000 years [in fact <2740 years].)
Realising that 1 million is 10^6 and "same weekday" amounts to working modulo 7 we can use Fermat's Little Theorem to immediately see that it will be the same weekday as tomorrow, clearly invaluable information...

Now it can also happen for *non-prime* n that $a^{n-1}\equiv 1 \pmod n$ (clear for $a=1$, and also for $a=-1$ and odd n; but also for composite n, e.g., $4^{14}\equiv 1 \pmod{15}$ or $13^{20}\equiv 1 \pmod{21}$). Nevertheless, one can give a characterization of primes using the above theorem, by also proving a converse:

Theorem: A natural number $p>1$ is prime if and only if *for all* a such that $a\not\equiv 0 \pmod p$ one has

$$a^{p-1}\equiv 1 \pmod p\,.$$

Proof: "only if": For p prime we know the statement from Fermat's Little Theorem.
"if": Suppose p is composite and satisfies the congruence above for all a not divisible by p; we can write it as $p=rs$ for some $r,s>1$, and by assumption as r is certainly not divisible by p (note $1<r<p$) we also get

$$r^{p-1}\equiv 1 \pmod p\,.$$

In particular we have $r\mid p\mid r^{p-1}-1$.
On the other hand, we have $r\mid r^{p-1}$, and so r divides the difference of the above, i.e., $=1$. This contradiction proves that a composite p cannot satisfy the condition in the Theorem. □

Carmichael numbers: If we slightly change the condition, by multiplying by a on both sides, the theorem would no longer be true: there are non-prime numbers,

so-called *Carmichael numbers*, for which $a^n \equiv a \pmod{n}$ *for all integers* a. The smallest such is $n = 561$. (There are in fact infinitely many of them—this was a longstanding conjecture, solved by Alford, Granville, Pomerance in 1994.)

Towards a "primality test". The above theorem will lead us to a good criterion to determine whether a number is "probably prime": try a selection of numbers $< p$ and check whether their $(p-1)$st powers are all $\equiv 1 \pmod{p}$, if they aren't, we know that the number is composite. On the other hand, it is rather unlikely that, for a *composite* p, a few (say ten) randomly selected such numbers have the property that all their $(p-1)$st powers are $1 \pmod{p}$, hence we can already say with high probability that the number p in question is a prime.

Another criterion to characterise primes is

Wilson's Theorem: For p a prime we have

$$(p-1)! \equiv -1 \pmod{p}\,.$$

Remark: In the exercises you are asked to prove that this is false for any *composite* $p > 4$.

Proof: For $p = 2$ the claim is obvious, and we assume now $p > 2$.

Idea: for each a with $0 < a < p$ we can find a solution of the linear congruence

$$ax \equiv 1 \pmod{p}\,.$$

⟦If you have seen $(\mathbb{Z}/p\mathbb{Z})^\times$, the group of *units* in $\mathbb{Z}/p\mathbb{Z}$, you can interpret x as the *inverse* of a in that group.⟧

There are two a in $(\mathbb{Z}/p\mathbb{Z})^\times$ which are their own inverses, i.e. for which $x = a$ solves the above: $a^2 \equiv 1 \pmod{p}$ implies $p \mid (a-1)(a+1)$ but in the given range this is only possible for $a = 1$ or $a = p-1$.

All the other a (i.e. $1 < a < p-1$) we can pair with an x such that $1 < x < p-1$ which solves the above congruence (i.e. x is the inverse of a), and so

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}\,,$$

since there are $(p-3)/2$ pairs (internally multiplying to $1 \pmod{p}$) which, when multiplied together, give the LHS.
It remains to multiply the equation by $p-1$. □

Example: Just to see how we can pair numbers off, take $p = 13$, where the inverses are as follows: $2 \cdot 7 \equiv 1$, $3 \cdot 9 \equiv 1$, $4 \cdot (-3) \equiv 1$, $5 \cdot (-5) \equiv 1$, $6 \cdot (-2) \equiv 1$, and of course 1 and -1 are their own inverses. So we get

$$(13-1)! \equiv \underbrace{(2 \cdot 7)}_{\equiv 1} \cdot \underbrace{(3 \cdot 9)}_{\equiv 1} \cdot \underbrace{(4 \cdot 10)}_{\equiv 1} \cdot \underbrace{(5 \cdot 8)}_{\equiv 1} \cdot \underbrace{(6 \cdot 11)}_{\equiv 1} \cdot 12 \pmod{13}\,,$$

hence $(13-1)! \equiv 12 \equiv -1 \pmod{13}$.

Remark: Note that, together with the above remark, Wilson's Theorem constitutes indeed another primality test—but an extremely inefficient one...

12. Lecture 11 (10.11.11)

Properties of $\varphi(n)$.
It is possible to evaluate Euler's φ-function rather quickly—*provided* we know the prime factorization of the number in question, due to the following properties:

- *Multiplicativity:* whenever $\gcd(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.
- *Prime powers:* For a *prime power* p^r (i.e. p is a prime and $r \geq 1$) we have $\varphi(p^r) = p^r - p^{r-1}$.

Proof: (Multiplicativity): We postpone the proof until after the one for the "Chinese Remainder Theorem".
(Prime powers): The only integers between 1 and n, for a prime power $n = p^r$, which are *not coprime* to n are the ones which are divisible by p, of which there are n/p, i.e. p^{r-1}, many.

Combining the above two properties we can get the following formula for $\varphi(n)$, any $n > 1$:

Proposition: If the positive integer n has the prime factorization $n = \prod_{i=1}^{k} p_i^{a_i}$ for some mutually different primes p_i and $a_i > 0$ $(i = 1, \ldots, k)$, then we have

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Proof: Using the fact that the primes are mutually different, hence coprime to each other, "multiplicativity" gives $\varphi(n) = \prod_{i=1}^{k}(p^{a_i} - p^{a_i - 1})$, which easily can be rewritten as the formula above. □

Chinese Remainder Theorem;
The problem of Sun Tzu, from "Sun Tzu Suan Ching" (translated e.g. as "Sun Tzu's Calculation Classic", ∼300 AD; cited from J. Silverman's book):

> We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?

Nowadays we would phrase the problem is follows: find $x \in \mathbb{Z}$ such that

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7. \end{aligned}$$

The so-called "Chinese Remainder Theorem" not only guarantees that this problem has a solution, its proof provides an algorithm to find it.

The Chinese Remainder Theorem: Let m, n be *coprime* positive integers and a, $b \in \mathbb{Z}$. Then there exists an $x \in \mathbb{Z}$ such that

$$\begin{aligned} x &\equiv a \pmod m \\ x &\equiv b \pmod n. \end{aligned}$$

Moreover, there exists a (unique!) solution x such that $0 \leq x < mn$.

Proof: Since m and n are coprime, we can find integers r and s such that

$$1 = rm + sn\,. \tag{3}$$

Multiplying both sides by a and by b, respectively, so we get

$$\begin{aligned} a &= arm + \underbrace{asn}\,, \\ b &= \underbrace{brm} + bsn\,, \end{aligned}$$

and then the sum $x = brm + asn$ of the "underbraced" expressions will do the trick: we have

$$x = brm + asn \equiv asn \equiv a \pmod{m}\,,$$

the last congruence due to (3), and similarly

$$x = brm + asn \equiv brm \equiv b \pmod{n}\,.$$

Moreover, there is a solution x with $0 \le x < mn$ (division by mn with remainder) and it is unique: suppose there is a second one x' satisfying the same congruences, then $x - x'$ is divisible by m and by n, hence also divisible by mn since $\gcd(m, n) = 1$, and hence $x - x'$ must be zero (as zero is the only number in the interval above which is divisible by mn). □

Here is another proof: The linear congruence

$$tm \equiv b - a \pmod{n}$$

has a solution t, since $\gcd(m, n) = 1$. In fact, there is a unique such solution t with $0 \le t < n$ (take the natural complete set of residues modulo n).
For this t with $0 \le t < n$ put $x = a + tm$. This solves both congruences in the theorem. ⟦Clearly $x \equiv a \pmod{m}$. But also $x = a + tm \equiv b \pmod{n}$.⟧

Successive application of this theorem allows us to solve Sun Tzu's problem:
in a first step, we use the theorem with $a = 2$, $b = 3$, $m = 3$ and $n = 5$. We write $1 = 2m + (-1)n$, and hence get

$$\begin{aligned} 2 &= 2 \cdot 2m + \underbrace{2(-1)n}\,, \\ 3 &= \underbrace{3 \cdot 2m} + 3(-1)n\,, \end{aligned}$$

and hence we find $x = 6m - 2n = 18 - 10 = 8$ which happens to already satisfy $0 \le x < 15$.
Applying now the Chinese Remainder Theorem for the simultaneous congruence

$$\begin{aligned} x &\equiv 8 \pmod{15} \\ x &\equiv 2 \pmod{7}\,. \end{aligned}$$

and multiplying $1 = 1 \cdot 15 + (-2) \cdot 7$ by 8 and 2, respectively, we find

$$\begin{aligned} 8 &= 8 \cdot 15 + \underbrace{8(-2)7}\,, \\ 2 &= \underbrace{2 \cdot 15} + 2(-2)7\,, \end{aligned}$$

and the sum of the underbraced terms $x = 30 - 112 = -82$ solves the problem. In order to get a positive solution, we need to add a multiple of $15 \cdot 7 = 105$, and we find $x = 23$. ⟦Of course, if one realises that one has to look for the same remainder

(=2) mod 3 and mod 7, then one could have seen that it is possible to combine them to the condition $x \equiv 2 \pmod{21}$ which would cut down one step, essentially.⟧

Multiplicative functions:

Definition: A function $f : \mathbb{N} \to \mathbb{Z}$ is called **multiplicative** if, for $\gcd(m, n) = 1$, one has

$$f(mn) = f(m)f(n)\,. \tag{4}$$

⟦A function $f : \mathbb{N} \to \mathbb{Z}$ is called **completely multiplicative** if for *any* m, n, one has (4).⟧

Example:

(1) For fixed k, the "raising to the k-th power" function f, defined by $f(n) = n^k$ is multiplicative, in fact even completely so.
(2) The "number of divisors" function $d(n) = \#\{g \geq 1 \mid g \,|\, n\}$ is multiplicative, but not completely so. The same holds for the "sum of divisors" function $\sigma(n) = \sum_{d|n} d$.
(3) For fixed k, the "taking gcd with k" function $f(n) = \gcd(n, k)$, is multiplicative but not completely so.

In particular, we want to see now (left from last week) that

Proposition: Euler's totient function is multiplicative.

Proof: Let m and n be coprime positive integers. Then consider the map

$$\{c \mid 1 \leq c \leq mn \text{ and } \gcd(c, mn) = 1\} \xrightarrow{f} \{a \mid 1 \leq a \leq m \text{ and } \gcd(a, m)\} \times \{b \mid 1 \leq b \leq n \text{ and } \gcd(b, n)\}\,,$$

where f is given by

$$f(c) = \big(c \pmod m,\ c \pmod n\big)\,.$$

If we can show that f is a bijection, then we have shown that both sides have the same size, the LHS being equal to $\varphi(mn)$, and the RHS equal to the product of $\varphi(m)$ (for the left factor) and $\varphi(n)$ (for the right factor).
Injectivity: Suppose $f(c) = f(c')$ for $1 \leq c, c' \leq mn$, then $c \equiv c' \pmod m$ and $c \equiv c' \pmod n$, i.e. both m and n divide $c - c'$; but then also mn does (as $\gcd(m, n) = 1$).
Surjectivity: For a coprime to m and b coprime to n we know from the Chinese Remainder Theorem that there is an integer c such that $c \equiv a \pmod m$ and $c \equiv b \pmod n$. Moreover, we can assume that $1 \leq c \leq mn$.
Finally, it is clear that c is coprime to m (as $c \equiv a \pmod m$) and to n (as $c \equiv b \pmod n$), hence also to their product mn, as $\gcd(m, n) = 1$.
This proves the bijection claim and hence the Proposition. □

13. Lecture 12 (11.11.11)

We can see that multiplicativity of φ and its simple evaluation for prime powers ($\varphi(p^k) = p^k - p^{k-1}$ for p prime) render it fairly easy to calculate, provided we know a factorization of the number in question.

Examples:
(i) $\varphi(20) = \#\{1, 3, 7, 9, 11, 13, 17, 19\} = 8$ can be calculated as $\varphi(4)\varphi(5) = 2 \cdot 4$.

(ii) $\varphi(10^4) = \varphi(5^4)\varphi(2^4) = (5^4 - 5^3) \cdot (2^4 - 2^3) = 5^3 \cdot 2^{2+3} = 32 \cdot 125 = 4000$.
(iii) $\varphi(4294049777) = \varphi(65521 \cdot 65537) = 65520 \cdot 65536$, as both factors are prime.

Modular exponentiation: Recall a previous
Theorem: A natural number p is prime if and only if for any a with $a \not\equiv 0 \pmod{p}$ one has

$$a^{p-1} \equiv 1 \pmod{p}\,.$$

In other words, we can prove that a number p is *composite* if we can show, for example, $2^{p-1} \not\equiv 1 \pmod{p}$, or $3^{p-1} \not\equiv 1 \pmod{p}$ etc. But even if a few such the congruences were true, we could *not* conclude that p is prime—nevertheless, the chances that p is prime would be already rather good.

This motivates already a need for a quick evaluation of $a^m \pmod{n}$ for large m. (We will see a further one shortly when dealing with "public key cryptography".)
The seemingly easiest way is to multiply a successively with itself, each multiplication followed by a reduction modulo n. But this would need $m-1$ multiplication steps and quickly becomes infeasible, even on a fast computer.
Instead, we devise a more clever way to break the calculations into only a few multiplications: take the binary expansion of the exponent, i.e., for some (sufficiently large) k we can
write $m = \varepsilon_k 2^k + \varepsilon_{k-1} 2^{k-1} + \cdots + \varepsilon_1 \cdot 2 + \varepsilon_0$, with $\varepsilon_i \in \{0, 1\}$.
Now all we need to know are the powers of a with exponent a power of 2, i.e. all a^{2^k}, $0 \le k < \log_2(m)$, and then a^m is the product of those powers a^{2^k} for which the coefficient ε_k above equals 1.

Example: Compute the last two digits of 6^{166}.
Solution: Write 166 in binary form, i.e. $166 = 128 + 32 + 4 + 2 = 2^7 + 2^5 + 2^2 + 2^1$ becomes $166 = (10100110)_2$.
hence $6^{166} = 6^{2^7} 6^{2^5} 6^{2^2} 6^{2^1}$ and so we only need to produce all the 2^k-th powers of 6 modulo 100, up to $k = 7$.
We produce the following table by successively dividing our original number m (here 166) by 2 and taking account of the remainders $\varepsilon_i \in \{0, 1\}$ at each step. Note that we only need to compute the squares 5 times, for any exponent (after this the sequence repeats periodically, as the last digit is always 6 and by Sheet 4, Q.1, squares ending in 6 have only 4 different possible remainders modulo 100).

k	m	ε_i	$6^{2^k} \pmod{100}$
0	166	0	6
1	83	1	36
2	41	1	96 ($= 36^2 = 1296 \mod 100$)
3	20	0	16 ($= (-4)^2 \mod 100$)
4	10	0	56 ($= 16^2 = 256 \mod 100$)
5	5	1	36 ($= (50+6)^2 \equiv 6^2 \mod 100$)
6	2	0	96 (as above)
7	1	1	16 (as above)

Putting those data back together, we obtain

$$\begin{aligned} 6^{166} &= 6^{2^7}6^{2^5}6^{2^2}6^{2^1} \equiv 16\cdot 36\cdot \underbrace{96}_{\equiv -4}\cdot 36 \pmod{100} \\ &\equiv 16\cdot(-4)\cdot \underbrace{36^2}_{\equiv 96} \equiv (-4)^2\cdot 16 \equiv 16^2 \pmod{100} \\ &\equiv 56 \pmod{100}. \end{aligned}$$

14. Lecture 13 (17.11.11)

We will study the following more difficult arithmetic

Questions: 1) Given a and $a^m \pmod n$, can we retrieve the exponent m *quickly*? 2) Given $a \pmod n$, can we take the mth root of a *quickly*?

Obviously, both questions can be solved in finite time, but the point is to find a *fast* method (provided it exists).

Today we concentrate on the first one, which leads to the *discrete logarithm problem.*

Definition: Let p be a prime and $a \in \mathbb{Z}$ with $(a,p)=1$. If $s \equiv a^m \pmod p$ for some m, then we call m the **discrete logarithm** of s (with respect to the prime p and the base a).

For real numbers, the logarithm is a continuous function and hence can be approximated numerically. By contrast, the discrete logarithm (with respect to some given prime and base) is very "jumpy", and we cannot expect to "approximate" it.

Discrete logarithm problem. *Fix p and a as above.*
Given s, devise a method to quickly *determine an m such that $s \equiv a^m \pmod p$.*

This problem is unsolved, and perhaps no such method exists.
In fact, the apparent unsolvability is in fact used for cryptographic purposes.

Public Key Cryptography

In this chapter, we discuss a rather surprising way to communicate with someone else which defies eavesdroppers who can intercept the messages. (E.g. think of two intimately befriended spies from different states who must be aware of the governments trying to intercept their messages; or, somewhat less dramatically, think of you communicating with your bank through online banking.)
Also, you want to make the transaction even more secure by possibly producing a different "shared secret code" each day to make it even harder for an eavesdropper to detect.

The idea is the following: once and for all the two parties, say Michael and Nikita (Mick'n'Nick?), agree (openly!) on a pair of positive numbers (p,g) where p is a prime and g an integer of order $p-1$ modulo p (i.e. the smallest positive k such that $g^k \equiv 1 \pmod p$ is $p-1$; note that for $k=p-1$ the congruence must hold by Fermat). ⟦We will see later that there are always plenty such numbers g, called "primitive roots modulo p".⟧

Then both Michael and Nikita choose (random) numbers m and n, respectively, both smaller than p, and send each other the numbers g^m and g^n, respectively (but *not* the numbers m and n).

They have to keep in mind that the eavesdropper (often personified as "Eve") will be able to intercept both g^m and g^n.
The "shared secret" code, which both Michael and Nikita are able to retrieve is

$$s := g^{mn} = (g^m)^n = (g^n)^m \pmod{p},$$

Michael knows m (which he chose) and g^n (which he was sent), but he need not know n, while Nikita knows n and g^m, but not m.

For reasonably large p (with 200 digits, say) it is practically impossible to retrieve g (which is unique, due to its having order $p-1$) from $g^m \pmod{p}$ and/or $g^n \pmod{p}$ (trying all the possibilities would take far too long).

Example: For $p = 11$ we know by Fermat that $g^{10} \equiv 1 \pmod{p}$), if coprime to p; we can find g of order 10 by checking that neither g^5 nor g^2 is 1 mod p (2 and 5 are the only non-trivial divisors of 10).
A quick check gives that $g = 2$ is a valid choice (neither $2^5 = 32 \equiv -1 \pmod{p}$ nor $2^2 = 4$ are $\equiv 1 \pmod{p}$).

Now Michael chooses (randomly) his secret $m = 6$, hence sends $g^m = 2^6 = 64 \equiv 9 \pmod{11}$ to Nikita.
Similarly, Nikita chooses (randomly) his secret $n = 7$, hence sends $g^n = 2^7 = 128 \equiv 7 \pmod{11}$ to Michael.
What is the shared secret?

Both can retrieve the shared secret code: Michael takes the number 7 he received and raises it to the power $m = 6$, so finds

$$7^6 = 343^2 \equiv 2^2 = 4 \pmod{11},$$

while Nikita takes the received number 9 and raises it to his chosen $n = 7$, and with the above modular exponentiation we find

$$9^7 \equiv (-2)^7 \equiv (-2) \cdot (-2)^2 \cdot (-2)^{2^2} = (-2) \cdot 4 \cdot 5 = -40 \equiv 4 \pmod{11}.$$

Hence indeed both results agree.

An eavesdropper would have to find m and n from the knowledge of p, g, g^m and g^n. This amounts to finding the exponent of g^m (or g^n), i.e. to solve the discrete logarithm problem for prime p and base g.

15. Lecture 14 (17.11.11)

Recall:

We had established a need for computing reasonably quickly the powers of a number g, say, modulo a modulus p (typically, but not necessarily, prime). As a first glimpse into the realm of cryptography we had encountered a scheme in which two people could establish a shared *secret key* by openly communicating data, and even if a party could intercept those data, they would still not be able to get the shared key!

The corresponding scheme is called the *Diffie-Hellman Key Exchange*. Here is how two parties (M and N, say) can establish a secret key:

i.) Either M or N determines a large (say, 200 digit) prime number p, together with an integer g of order $p-1$ modulo p. Both p and g can be made *public*.

ii) M chooses a *secret* random integer m with $1 \leq m \leq p-2$.
N chooses a *secret* random integer n with $1 \leq n \leq p-2$.
iii) M sends $g^m \pmod p$ to N.
N sends $g^n \pmod p$ to M.
iv) Both can now calculate the shared *secret* key given by $s := g^{mn} \pmod p$.

The *security* of the key depends on the fact that, given p, g and $g^m \pmod p$, it is in general unfeasible to find m.

The above scheme was published in 1976 by Diffie and Hellman. Now GCHQ
http://www.amazon.co.uk/GCHQ-Richard-Aldrich/dp/0007278470
turned out to have found a very similar procedure a few years earlier—but since the information about it was classified, they were not able to claim priority...
The scheme is a "concept" rather than a "realization". We will see one such shortly (keyword "RSA algorithm").

Computing k^{th} roots modulo an integer. We also will have a need to perform the *inverse* to the powering modulo p, i.e., to take the k^{th} *root* modulo an integer. For example, how can we find a cube root of $19 \pmod{11}$? As a congruence, the problem reads

$$x^3 \equiv 19 \pmod{11},$$

and if we realise that $19 \equiv 8 \pmod{11}$, a solution becomes obvious (take $x = 2$).

In the case above, a quick test taking the cubes for $x = 0, 1, \ldots, 10$ modulo 11 ⟦why are these 11 numbers sufficient?⟧ reveals that 2 is the unique(!) solution.

But the above method would be much more cumbersome for the problem of solving

$$x^{101} \equiv 262 \pmod{667}, \tag{5}$$

for instance.

A far better method to do it is by using the Euclidean algorithm, combined with Euler-Fermat. First compute $\varphi(667)$, which, due to the prime decomposition $667 = 23 \cdot 29$, is equal to $22 \cdot 28 = (25-3)(25+3) = 625 - 9 = 616$ (or better decompose it into prime factors: $616 = 2^3 \cdot 7 \cdot 11$).

If our exponent, here 101, is coprime to $\varphi(667)$ (clear since 101 is prime and leaves remainder 10 modulo 616), then we can solve the equation

$$1 = a \cdot 101 + b \cdot 616$$

by the corollary to the Euclidean algorithm (sometimes also called *extended Euclidean algorithm*), say; one solution is $a = 61$, $b = -10$, as one can easily check (try it in your head, actually!).

Now we are ready to "solve for x" in (5): by the above and Euler-Fermat we find

$$x = x^1 = x^{61 \cdot 101 - 10 \cdot 616} \equiv x^{61 \cdot 101} = (x^{101})^{61} \pmod{667}$$

and inserting (5) we get

$$x \equiv 262^{61} \pmod{667},$$

which we can solve using our method of successive squaring from last time (giving $233 \pmod{667}$).

Summary of the above: we can compute the k^{th} roots modulo a number m, *provided* we can find $\varphi(m)$. More precisely, one has the

Algorithm for computing k^{th} roots modulo m.
Given $m > 1$, let r be coprime to m, and let k be coprime to $\varphi(m)$.

Then we can solve the congruence

$$x^k \equiv r \pmod{m}.$$

More precisely, we can do it in the following way:

1) Compute $\varphi(m)$.
2) Find positive integers a and b such that $1 = ak - b\varphi(m)$.
3) Compute $r^a \pmod{m}$, using the method of successive squaring. This gives our desired x.

The RSA algorithm. The innocuous–looking provision in the above summary (to find $\varphi(m)$) is crucial; it essentially amounts to *factoring* m, which is considered to be *very hard* in general.
Therefore, if we choose m suitably, then we can *openly* communicate how anybody can encode a message but only people who know how to factor m will be able to decode. This discrepancy is the basis of the RSA cryptosystem:

Crucial idea: a "trapdoor function". This is a simple albeit not quite well-defined concept. A *trapdoor/ one-way function* on a set X is an invertible map $E : X \to X$ such that E^{-1} can be computed easily, provided one has some *extra information*, but extremely hard if one doesn't.

Example: An example of a trapdoor function E can be concocted as follows:

(1) Choose two different large primes p and q (say, 100 digits long each) and take $n = pq$ (the "RSA modulus").
(2) Choose a positive number (an "encryption" exponent) $e < \varphi(n)$ which is *coprime to* $\varphi(n)$.
(3) Define $E : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $E(x) = x^e \pmod{n}$.

Why is this considered a trapdoor function?

- On the one hand, it is easy to invert E, provided we can find d such that $de \equiv 1 \pmod{\varphi(n)}$, in view of our previous subsection (computing k^{th} roots modulo an integer, here $k = e$ and the integer n). But there we have seen that for this all we need to know is the *extra information* $\varphi(n)$ itself. By concocting n as in (1) we get $\varphi(n)$ for free.
  The inverse function E^{-1} is given by $E(x) = x^d \pmod{n}$, and d is called the "decryption" exponent.
- On the other hand, determining d from n and e amounts essentially to determining $\varphi(n)$ which is extremely hard for a typical n in question *without* knowing the prime decomposition of the latter.

From this trapdoor function, we produce a *public key* (n, e), a pair of integers as above, which allows everybody to encode their message m by raising it to the e^{th} power modulo n (we have seen that this can be done rather quickly).

Specific example.
Problem: Suppose our RSA modulus is $n = 55$ and our exponent is $e = 3$.
Find the decryption exponent d.

Solution: We first find $\varphi(55) = \varphi(5)\varphi(11) = 4 \cdot 10 = 40$, then write $1 = a \cdot 3 - b \cdot 40$, e.g. we find $a = 27$, $b = 2$ (by inspection or by Euclidean algorithm).
Hence the decryption exponent is $d = 27$.

How to encode a message? Suppose we want to write a telegram message and transform it into a number in a simple way; then a standard method is to simply take the usual bijection between the letters A, B, C, ..., Z of the alphabet and the numbers 1, 2,..., 26. We can also add a blank and identify with 0, then we can transform any message (ignoring punctuation) into a (possibly long) number.

Example. We can work in base 27 (or any base ≥ 27) to make sure that the alphabet can be embedded injectively.
We have the following correspondence:

$$D \leftrightarrow 4\,, \qquad U \leftrightarrow 21\,, \qquad R \leftrightarrow 18\,, \qquad H \leftrightarrow 8\,, \qquad A \leftrightarrow 1\,, \qquad M \leftrightarrow 13\,,$$

from which we produce the decimal expansion of the number

$$4 + 27 \cdot 21 + 18 \cdot 27^2 + 8 \cdot 27^3 + 1 \cdot 27^4 + 13 \cdot 27^5 = 187238389\,,$$

our numerical equivalent of DURHAM.

If we want to retrieve the digits in base 27 from this, it suffices to repeatedly divide by 27 and take the remainders:

$$\begin{aligned} 187238389 : 27 &= 6934755 \text{ remainder } 4 \\ 6934755 : 27 &= 256842 \text{ remainder } 21 \\ 256842 : 27 &= 9512 \text{ remainder } 18 \\ 9512 : 27 &= 352 \text{ remainder } 8 \\ 352 : 27 &= 13 \text{ remainder } 1 \\ 13 : 27 &= 0 \text{ remainder } 13\,, \end{aligned}$$

which we can then translate back with our bijection (alphabet $\leftrightarrow$ 1,...,26) into the original message.

16. Lecture 15 (24.11.11)

Description of the RSA. Finally we can put our knowledge together to formalise the *RSA algorithm:*

1. Nikita chooses two large primes p and q and produces $n = pq$.
2. Nikita also chooses an exponent e coprime to $\varphi(n) = (p-1)(q-1)$.
3. Nikita computes an inverse d of e in $\mathbb{Z}/\varphi(n)\mathbb{Z}$.
4. Nikita makes the key (n, e) public.
5. Michael encodes a message m as $m^e \pmod n$, sends it to Nikita.
6. Nikita decodes the message m^e by computing $(m^e)^d \pmod n$.

Simple example: Small numbers, very short message, to concentrate on the concept (clearly not a safe encoding).

1. We choose $p = 17$, $q = 19$, so that $pq = 18^2 - 1 = 323$. We easily determine $\varphi(n)$ simply as $(17-1)(19-1) = 16 \cdot 18 = 17^2 - 1 = 288$.
2. Now choose an e coprime to 288, say $95 (= 5 \cdot 19)$.
3. Find an inverse of 95 modulo 288 (use extended Euclidean algorithm) as 191.
4. Our public key is $(323, 95)$.

5. Someone encodes the letter "X", which is identified with its numerical equivalent 24 (the third-to-last letter in the alphabet [of length 26]), and encodes it as $24^{95} \pmod{323}$, as the public key requires. It turns out to be 294 (mod 323) which he sends to us.
6. We decode this message 294 by computing $294^{191} \pmod{323}$ which indeed becomes 24.

For longer messages, one can e.g. transmit each letter in a similar way, so e.g. one could send the sequence F,O,X as $309(= 6^{95})$, $059(= 15^{95})$, $294(= 24^{95})$.

Note that such a method is rather unsafe. It is much better to put several letters together and send them as a block.

Recall: last time's encryption method consists roughly of the following steps:

1. each letter of the alphabet is translated into a number;
2. each number m is encryptd using a public key (n, e) [with n our RSA modulus, e an encryption exponent modulo n], i.e. by $m^e \pmod{n}$.

How safe is our encryption method? Note that the way we used the above encryption method is rather unsafe; an eavesdropper can use frequency analysis and compare, say, with the public tables listing the average frequency of letters in the English language—e.g. about every eighth letter is an e, every eleventh is a t, then a (0.082), o (0.075) and i (0.07) follow (cf. e.g., Trappe/Washington, Table 2.1, p.17), and with a bit of effort plus trial and error Eve could detect the key.

Improvement: It is much better to put several letters together and send them *as a block*.

Example: Suppose we want to encode a message using the usual bijection between letters of the alphabet and the numbers "01", ..., "26", so e.g. the message "FLEE" (the *plaintext*) becomes "06120505" (let us call this the *codetext*).

Now depending on the public key (n, e) we may have to cut the message into blocks before sending it. (Otherwise, there is a danger that several messages are encoded as the *same* number modulo n.)

If the RSA modulus n is 9 digits long, say $10007 \cdot 10009$ (= 100160063), then we can send blocks of 4 such. Of course we don't just send the codetext as is, but rather encrypt it by raising it to some power e, say $e = 17$, by which process it becomes the *ciphertext*.

- plaintext "FLEE";
- becomes "06120505" (our codetext);
- ciphertext $06120505^{17} \pmod{100160063}$,
  i.e. $69808849 \pmod{100160063}$;

Now if we want to decrypt, we simply have to raise to the decryption exponent mod n; if we realise that $\varphi(n) = 10006 \cdot 10008$ (n is the product of two primes), then we find $d = 94249457$ using the Euclidean algorithm. So to decrypt 69808849, we calculate $69808849^{94249457} \pmod{100160063}$ which turns out to be 6120505, to which we can then add a "0" on the left to make the number of digits even, and then we interpret the blocks of 2 digits as letters (in reverse to the above).

Possible factorization methods ("attacks") for an RSA modulus:
In the following, suppose we have $n = pq$, the number of two primes p and q.

Proposition: If we know n and $\varphi(n)$, we can easily factor n.

Proof: We know that $\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1$, hence

$$p + q = n - \varphi(n) + 1\,.$$

Now p and q are the roots of the quadratic equation

$$0 = (x-p)(x-q) = x^2 - (p+q)x + pq = x^2 - (n - \varphi(n) + 1)x + n\,.$$

But then we can solve the quadratic equation... □

Example: Suppose we know that $n = 437$ is the product of two primes and $\varphi(n) = 396$.
Then we find the roots of

$$x^2 - \underbrace{(n - \varphi(n) + 1)}_{=42}\, x + 437$$

are given by

$$x = 21 \pm \sqrt{21^2 - 437} = 21 \pm 2\,.$$

Hence $437 = 19 \cdot 23$.

Claim: If p and q are "close", then we can find a factorization of n.
A procedure to find this is called the "Fermat factorization method".

The idea behind it is as follows: we can assume $p > q$ (if $p = q$ it would be even easier); now by assumption $s := \frac{p-q}{2}$ is small compared to $t := \frac{p+q}{2}$ which is close to $\sqrt{n}$; moreover, we can find n as the difference of their squares:

$$t^2 - s^2 = \Big(\frac{p+q}{2}\Big)^2 - \Big(\frac{p-q}{2}\Big)^2 = \frac{1}{4}\big(p^2 + 2pq + q^2 - (p^2 - (2pq) + q^2)\big) = pq = n\,.$$

Therefore, we can test whether $t^2 - n$ is a square, for t close to (and larger than) $\sqrt{n}$, and try $t = \lceil\sqrt{n}\rceil$, $t = \lceil\sqrt{n}+1\rceil$, $t = \lceil\sqrt{n}+2\rceil$, etc. until $t^2 - n$ indeed becomes a square. Here $\lceil x\rceil$ denotes the smallest integer larger than or equal to x.

Example: Take $n = pq$ with the primes $p = 1201$ and $q = 1409$. This gives $n = 1692209$, and, in GP-PARI notation, `t=floor(sqrt(n))+1` becomes 1301;
Now trying the next t (by adding 1 and then testing $\sqrt{t^2 - n}$), i.e.

```
t=t+1;sqrt(t^2-n)
```

produces 54.726593170048507962879261 82;
repeated application of this gives successively
$74.8331477\ldots$, $90.5924941\ldots$, $104.0000000\ldots$; the latter looks like an integer, so we put $s = 104$, which then provides 1305 (the current t, as we've added "1" four times to our original t) and so we get the factorization $t^2 - s^2 = (t-s)(t+s) = 1409 \cdot 1201$.

17. Lecture 16 (25.11.11)

Factoring an RSA modulus "with high probability": It turns out that, for the RSA algorithm attached to the public key (n, e), to find the decryption key d is essentially as difficult as to factor the modulus n, in the following sense.

Suppose we have obtained d by some means, so we know n, e and d but we do not have the factorization of n.

Then we can factor n "with high probability":

A first observation is that we have found an exponent m such that $a^m \equiv 1 \pmod{n}$ for all a with $\gcd(a, n) = 1$: take $m = de - 1$.

A second observation is that this m is even: take $(-1)^m \pmod n$ which by the previous step is 1, whence m is even.
Now the *main idea* is to compute the successive "square roots" of $a^m \pmod n$, i.e. $a^{m/2} \pmod n$, $a^{m/4} \pmod n$, ..., until one of these roots $a^{m/2^k} \pmod n$ is $\not\equiv 1 \pmod n$. (If this does not occur for any k for which $m/2^k$ is an integer, we pass to another a.)
Now there is a good (about 50%) chance that this a satisfies, for $m' := m/2^k$ in the above,

$$a^{m'} \equiv 1 \pmod p\,, \qquad a^{m'} \equiv -1 \pmod q$$

or (equivalent by symmetry)

$$a^{m'} \equiv -1 \pmod p\,, \qquad a^{m'} \equiv 1 \pmod q\,.$$

In either of these two cases we find a proper divisor of n (and by the assumption $n = pq$ in fact already a factorization of n) by computing a gcd, which we know is "cheap"/"easy": e.g. in the first case we find

$$p \mid a^{m'} - 1\,, \qquad \text{and} \quad q \nmid a^{m'} - 1$$

and therefore

$$\gcd(a^{m'} - 1, pq) = p\,,$$

which gives a divisor of n.
In case this a did not yield such a pair of congruences for any possible choice of m', we pick another a at random... We will almost certainly succeed within a few trials.

Example: Suppose we are given the modulus $n = 10403$, encryption exponent $e = 7$ and our spy informs us that $d = 8743$ is the decryption key. We want to find the factorization of n.
We try $a = 5$, and find that
$m = de - 1 = 61200$.
For $k = 1$, 2 or 3 we find that $a^{m/2^k} \equiv 1 \pmod n$, while for $k = 4$ we get
$m/2^4 = 3825$ and $a^{3825} \equiv 102 \pmod n$.
Now we compute $\gcd(a^{3825} - 1, n) = 101$ which is very fast (for a computer), despite the fact that 5^{3825} has more than 2600 digits, revealing again the power of the Euclidean algorithm!
But we actually need not compute the actual value of $a^{3825} - 1$ (this would be soon impractical for larger exponents): it suffices to work modulo n.

If we had tried $a = 2$, we would have found $\gcd(2^{m/8} - 1, n) = 103$, i.e. the other prime dividing n.
(For a more detailed discussion of this, see Stein's book, §3.4.3.)

Primitive roots modulo a prime. One of the results we have (implicitly) used so far without proving it is that *for each prime p there is always an integer m of* order $p - 1$. We will elaborate on this property now, recalling a few preliminaries.

(1) In Algebra, (most of) you have seen that $\mathbb{Z}/p\mathbb{Z}$ is a field, if p is prime. We know how to add and multiply, how to take negatives (i.e. inverses w.r.t. addition) and we know how to invert non-zero elements.
⟦If you haven't seen this, then simply check that each non-zero element a has an inverse by using the extended Euclidean algorithm to write $1 = xa + yp$

to find the inverse of a as the class of x modulo p.⟧
In particular, we find that the set of non-zero elements form a *group*, in fact an *abelian* one.

(2) Moreover, you have seen in that same course that a non-zero polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with coefficients a_j in a field F has at most n roots in F.
(3) Fermat's Little Theorem immediately implies that there are $p-1$ different roots modulo p of the polynomial $x^{p-1} - 1$.

We generalise the latter result in our context:

Proposition: For a prime p and a divisor d of $\varphi(p)$, the polynomial $f(x) = x^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ has *precisely* d (different) roots in $\mathbb{Z}/p\mathbb{Z}$.

Proof: Putting $e = \varphi(p)/d$, an *integer*, we have

$$\begin{aligned} x^{p-1} - 1 &= (x^d)^e - 1 \\ &= (x^d - 1)((x^d)^{e-1} + (x^d)^{e-2} + \ldots + x^d + 1)\,, \end{aligned}$$

hence we can write $x^{p-1} - 1 = (x^d - 1)g(x)$ for some polynomial $g(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ of degree $d(e-1) = p - 1 - d$.
Now by (1) above we know that $g(x)$ has *at most* $p - 1 - d$ roots, and also that $x^d - 1$ has *at most* d roots. But the left hand side has precisely $p - 1$ roots by (3) above, so we can replace "at most" by "precisely" in both cases.
⟦From $p - 1 = \underbrace{\deg(x^d - 1)}_{\geq d} + \underbrace{\deg(g(x))}_{\geq p-1+d} \geq d + (p - 1 - d) = p - 1$ we find that in fact equality must hold in place of "$\geq$".⟧
Conclusion: The polynomial $x^d - 1$ with $d \mid p - 1$ has precisely d different roots modulo p. □

18. Lecture 17 (1.12.11)

Recall:
Proposition: For a given prime p and a divisor d of $\varphi(p)$, the polynomial

$f(x) = x^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ has *precisely* d (different) roots in $\mathbb{Z}/p\mathbb{Z}$.

Example: For $p = 11$ we have two non-trivial divisors of $\varphi(p) = 10$, viz. $d_1 = 2$ and $d_2 = 5$.
For $x^{d_1} - 1$ we find easily the two roots $x = \pm 1$, and the above proposition tells us that these are the only solutions.
For $x^{d_2} - 1 = x^5 - 1$ the same proposition tells us that we should be able to find five different solutions: indeed we find that 1^5, 3^5, 4^5, 5^5 and 9^5 are all $\equiv 1 \pmod{11}$, so the classes of 1, 3, 4, 5 and 9 in $\mathbb{Z}/11\mathbb{Z}$ are the solutions. (All the other five non-zero classes, raised to the fifth power, are actually $\equiv -1 \pmod{11}$.)

The structure of the units in $\mathbb{Z}/p\mathbb{Z}$

We need to recall/introduce a further notion.

Definition: Fix a prime p. The *order* of an element $a \in \mathbb{Z}$ modulo p, where a is coprime to p, is the *smallest positive* exponent m such that

$$a^m \equiv 1 \pmod{p}\,.$$

We denote this m by $\mathrm{ord}_p(a)$, the "order of a modulo p".

Why does such an m exist at all? Clearly, Fermat's Little Theorem tells us that $p-1$ will be such an exponent, albeit not necessarily the smallest positive one.
[Even if we didn't know Fermat, we could see the existence by arguing as follows: If we write a list of powers of a modulo p, i.e. $a \pmod p, a^2 \pmod p, a^3 \pmod p, \ldots$, then it is clear that there must be repetitions, as there are only finitely many (in fact, p) different residues modulo p. So there must be two integers i and j, $(i > j)$ for which $a^i \equiv a^j \pmod p$. But we can cancel a from both sides, since $\gcd(a,p) = 1$, in fact we do this j times to get $a^{i-j} \equiv 1 \pmod p$.]

Note that a completely analogous definition can be used for any integer in place of p; moreover, one can extend it to any group—with the slight modification that we call the order of an element a in a group *infinite* if there is no such exponent m.

Definition: For any prime $p \geq 2$, a *primitive root* modulo p is an integer a, coprime to p, of *maximal* order (i.e. order $p-1$ modulo p).

Example: Let $p = 7$ and $a = 3$. Then a is a primitive root modulo 7:

$$3^1 \equiv 3\,, \qquad 3^2 \equiv 2\,, \qquad 3^3 \equiv 6\,, \qquad 3^4 \equiv 4\,, \qquad 3^5 \equiv 5\,, \qquad 3^6 \equiv 1 \pmod 7\,.$$

On the other hand, 2 is *not* a primitive root modulo 7, since already $2^3 \equiv 1$. There is nevertheless another primitive root modulo 7, given by $a = 5 \equiv -2$.

A first remark: we know from Fermat that, for any a coprime to p, we have that $\mathrm{ord}_p(a) \leq p-1$. What is more, we now first establish the following "order divisibility property": the order of a modulo p has to *divide* $p-1$.

Proposition. Let $a \in \mathbb{Z}$ be coprime to the prime p such that $a^n \equiv 1 \pmod p$. Then

$$\mathrm{ord}_p(a) \mid n\,.$$

In particular, $\mathrm{ord}_p(a) \mid p-1$.

Proof: Let $e = \mathrm{ord}_p(a)$, i.e. e is the *smallest* positive exponent m for which $a^m \equiv 1 \pmod p$; then we have both

$$a^e \equiv 1 \pmod p\,, \qquad a^n \equiv 1 \pmod p\,.$$

Let $g = \gcd(e,n)$. We want to show that $g = e$ since then e is a divisor of n.
So assume for a contradiction that $g < e$, then we can write $g = x \cdot e + y \cdot n$ for some integers x, y, and then we find

$$a^g = a^{xe+yn} = (a^e)^x \cdot (a^n)^y \equiv 1 \pmod p\,,$$

contradicting the minimality of e.
Hence we indeed conclude that $g = e$, and in particular $e \mid n$. □

We will see the following "summation formula for φ".
Exercise: Let d_1, d_2, …, d_r the (positive) divisors of $n \geq 1$. Then

$$\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_r) = n\,.$$

This leads us now to the

Theorem. ("Existence of a primitive root modulo p"). Every prime p has a primitive root modulo p.
Moreover, there are precisely $\varphi(p-1)$ primitive roots modulo p.

Proof: For any divisor n of $p-1$ we find precisely n solutions in $\mathbb{Z}/p\mathbb{Z}$ of the polynomial $x^n - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ (proposition from last time).

On the other hand, we know by the above order divisibility property that each such solution a of $x^n - 1 = 0$ (in particular a is coprime to p) has an order modulo p which is a *divisor* of n (and hence, by transitivity of divisibility, also of $p-1$).
Therefore we can group these solutions according to their order e, into sets

$$S_p(e) := \{1 \leq a \leq p-1 \mid \mathrm{ord}_p(a) = e\}\,,$$

and we will list all of the roots of $x^n - 1$ if we take the union

$$\bigcup_{d|n} S_p(d)\,,$$

(note that we could just as well take the union over all $1 \leq d \leq p-1$, but that then several of the sets $S_p(d)$ would be empty).
Now each residue class a occurs in precisely *one* such set (due to the fact that the order of a is well-defined), so this union is a disjoint one. Hence if we put, for any $d \geq 1$,

$$\psi(d) = \#S_p(d) = \#\{1 \leq a \leq p-1 \mid \mathrm{ord}_p(a) = d\}\,,$$

then we find, again denoting by $d_1, \ldots, d_r$ the divisors of n, that

$$n = \psi(d_1) + \cdots + \psi(d_r) = \sum_{d|n} \psi(d)\,.$$

Using this, together with above exercise, we can now show by induction that ψ and φ define the same function, i.e. $\varphi(n) = \psi(n)$ for any $n \geq 1$:
The statement is clear for $n = 1$, where both $\varphi(1)$ and $\psi(1)$ equal 1.
Suppose now we have proved the statement for any $d < n$. Then we find, putting wlog. $n = d_1$, that

$$\psi(n) + \psi(d_2) + \cdots + \psi(d_r) = n = \varphi(n) + \varphi(d_2) + \cdots + \varphi(d_r)\,,$$

but $d_j < n$ $(2 \leq j \leq r)$, as all these d_j are *proper* divisors of n, and so by assumption also $\psi(d_j) = \varphi(d_j)$ $(2 \leq j \leq r)$, hence we can conclude $\psi(d_1) = \varphi(d_1)$, i.e. $\psi(n) = \varphi(n)$.

Conclusion: we have proved that for any n dividing $p-1$ there are precisely $\varphi(n)$ integers a modulo p such that $\mathrm{ord}_p(a) = n$.
Now consider the special case $n = p-1$: we find that indeed there must be precisely $\varphi(p-1)$ integers of order $p-1$ modulo p, in other words *primitive roots* modulo p. □

Corollary: The group $(\mathbb{Z}/p\mathbb{Z})^\times$ is a *cyclic* group, i.e. it is generated by a single element.
⟦**Proof:** Follows immediately from the theorem, in fact we have $\varphi(p-1)$ different elements which can serve as a generator.⟧

While the theorem gives us an idea *how many* such primitive roots exist, it does not say how we can find a particular one. For example, $a = 2$ is primitive root modulo $p = 3, 5, 11, 13, 19, 29, \ldots$, but *not primitive* modulo $p = 7, 23, 31, \ldots$.
Note: one does not expect a simple pattern here...

In fact, we have a famous unproven conjecture:

Artin's Conjecture. There are infinitely many primes p for which 2 is a primitive root modulo p.

More generally, one has a similar conjecture ("Generalized Artin Conjecture") for any non-square $a > 2$ in place of 2 above.

An amazing result in support of this conjecture was found by Gupta, Ram Murty, and Heath-Brown (1985): There are *at most three* pairwise coprime a for which the Generalized Artin Conjecture is *false*...
⟦No-one has been able so far to exclude $a = 2$ as one of the three, hence Artin's original conjecture is still unsolved.⟧

19. Lecture 18 (2.12.11)

The discrete logarithm and the index.
Suppose we have chosen a primitive root g modulo a prime p (there are plenty such, as we have seen, more precisely $\varphi(\varphi(p))$ many). We denote it by g to remind ourselves that it *generates* the group $(\mathbb{Z}/p\mathbb{Z})^\times$. The crucial property of such a g is that, for any $a = 1, \dots, p-1$, there is *precisely one* power g^r, for some $r = 1, \dots, p-1$ (depending on a, obviously) such that $a \equiv g^r \pmod p$. In other words, the set

$$\{g \pmod p,\ g^2 \pmod p,\ g^3 \pmod p,\ \dots\ ,\ g^{p-1} \pmod p\}$$

is, as a *set*, is simply $\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$.

Definition: We call r as above (i.e. with $a \equiv g^r \pmod p$) the *index of a modulo p for the base g*.
Our notation will be $I(a) := I_{p,g}(a) = r$. Note that it depends on *both* p and g.

Note: For given p and primitive root g for p, we have

$$g^{I(a)} \equiv a \pmod p\,.$$

Hence we can think of I as the *inverse function* of exponentiating (more precisely, of exponentiating the base g modulo p).

In our example from last time, we can reorder the list we obtained, and write:

Example: Let $p = 7$ and $g = 3$.

$$1 \equiv g^6\,, \qquad 2 \equiv g^2\,, \qquad 3 \equiv g^1\,, \qquad 4 \equiv g^4\,, \qquad 5 \equiv g^5\,, \qquad 6 \equiv g^3 \pmod 7\,.$$

Hence we can read off the index of 6 modulo 7 with respect to the base $g = 3$ as the exponent 3.

Q.: But is there any pattern in this above list? For example, given $a = 6$, is there a formula, or at least a reasonably fast algorithm that finds the corresponding exponent 3 above, different from the naive one which is going through the list?
A.: For general p and g, no such formula or algorithm is known! The underlying problem is a rather famous one, which goes by the name of the *discrete logarithm problem*.

In order to motivate the name, recall the *classical logarithm* to a base b (with $b \in \mathbb{R}_{>0}$, say), which essentially amounts to "detecting the exponent x" (for some $x \in \mathbb{R}$) of a given $a \in \mathbb{R}_{>0}$ in the equation

$$b^x = a\,.$$

This logarithm satisfies the "functional equation"

$$\log_b(a_1 a_2) = \underbrace{\log_b(a_1)}_{=:\ell_1} + \underbrace{\log_b(a_2)}_{=:\ell_2}\,,$$

which merely restates the fact that adding exponents ℓ_1, ℓ_2 amounts to multiplying the exponentiated numbers

$$b^{\ell_1+\ell_2} = b^{\ell_1} \cdot b^{\ell_2}\,.$$

This latter property is of course still true if we work with integers b, ℓ_1, ℓ_2, and it holds even if we consider only congruences instead. In our example above we find

$$g^3 \cdot g^4 \equiv 6 \cdot 4 \equiv 3 \equiv g^1 \pmod 7\,,$$

(still $g = 3$), and for the exponents, i.e., the *discrete logarithms*, we therefore would find that $3 + 4 = 1$. This is true if we *work modulo* 6.
Indeed, since we know that $g^{p-1} \equiv 1 \equiv g^0 \pmod p$, we should, for general p, *work modulo* $p - 1$ *in the exponent*.

The following rules apply for the indices (for chosen p and g):
Proposition: For a_1, a_2, $k \in \mathbb{Z}$, we have

- $I(a_1a_2) \equiv I(a_1) + I(a_2) \pmod{p-1}$, [product rule]
- $I(a^k) \equiv k \cdot I(a) \pmod{p-1}$. [power rule]

⟦The **proof** consists simply in reworking the definition, e.g. for the product rule we raise the base g to the power of each side

$$g^{I(a_1a_2)} \equiv a_1a_2\,, \qquad g^{I(a_1)+I(a_2)} = g^{I(a_1)} \cdot g^{I(a_2)} \equiv a_1 \cdot a_2 \pmod p\,,$$

which clearly agree, and so $g^{I(a_1a_2)-I(a_1)-I(a_2)} \equiv 1 \pmod p$. Hence, since the order of g (with respect to p) is $p-1$, we must have that $p-1 \mid I(a_1a_2) - I(a_1) - I(a_2)$.⟧

Now if we have a table of indices given, for fixed p and g, then we can solve even harder problems than before: consider the table for $p = 11$ and $g = 2$ given by

a	1	2	3	4	5	6	7	8	9	10
$I(a)$	10	1	8	2	4	9	7	3	6	5

This table is interpreted as follows: for $a = 6$ we find $I(a) = 9$, so we should have $2^9 \equiv 6 \pmod{11}$. (Indeed, $2^9 - 6 = 512 - 6 = 506$ which can be readily seen to be divisible by 11.)

Then we can solve an equation like

$$x \equiv 8^{103} \pmod{11}$$

by computing indices (note that we work modulo $p - 1$ here, since we deal with *exponents*!):

$$I(x) = I(8^{103}) = 103 \cdot I(8) = 103 \cdot 3 \equiv 3 \cdot 3 \equiv 9 \pmod{10}$$

and so (note that we now work modulo p again)

$$8^{103} \equiv g^{I(8^{103})} \equiv g^9 = 6 \pmod{11}\,.$$

Example 1: Another, slightly more complicated example is to find a solution of

$$9x^3 \equiv 8 \pmod{11}$$

by passing to indices: we find

$$I(9x^3) = I(9) + 3I(x) \equiv I(8) \pmod{10}$$

i.e. $6 + 3 \cdot I(x) \equiv 3 \pmod{10}$, for which we can easily find a solution $I(x) = 9$, hence $x = 6$.

Example 2: Now suppose we try to solve the equation

$$3x^{11} \equiv 25 \pmod{37}, \tag{6}$$

where someone has told us that for $p = 37$ and $g = 2$ one has

$$I(3) = 26, \qquad I(4) = 2, \qquad I(5) = 23.$$

Then we can solve (6) above, working modulo $p - 1 = 36$:

$$\begin{aligned}
I(3x^{11}) &\equiv I(25), && \text{by taking indices,}\\
I(3) + 11 \cdot I(x) &\equiv I(5^2) = 2 \cdot I(5), && \text{by expanding,}\\
26 + 11 \cdot I(x) &\equiv 2 \cdot 23, && \text{plugging in the indices above,}\\
11 \cdot I(x) &\equiv 20, &&\\
I(x) &\equiv 23 \cdot 20, && \text{using that } 23 \cdot 11 = 253 = 36 \cdot 7 + 1\\
I(x) &\equiv 460 \equiv 28 \pmod{36}. &&
\end{aligned}$$

Now if we knew all the entries in the table, we could simply look up x such that $I(x) = 28$. But we can get by with the 3 values above in our case, as

$$28 = 26 + 2 \equiv I(3) + I(4) \pmod{36}$$

and, using the product rule, we can write the latter as $I(12)$.
Conclusion: $x = 12$ solves the above equation.

The discrete logarithm problem and secure encryption. Recall that in the Diffie-Hellman key exchange protocol two communicating parties agree on a pair (p, g) where p is a prime and g a primitive root modulo p, and both sides choose an exponent m and n, respectively, in order to create the shared secret key g^{mn}. Since the information g^m (resp. g^n) is transmitted over a *public* channel, and since moreover both p and g are publically known, a third party could retrieve the shared secret *if* they could retrieve m from the knowledge of p, g and $g^m \pmod p$, i.e. *if* they could solve the discrete logarithm problem as stated above. The fact that nobody has found a feasible algorithm for it guarantees [at least for now] the security of this encryption method and similar ones (google, for example, the "ElGamal" public key encryption).

20. Lecture 19 (8.12.11)

Squares modulo a prime p. In the problem sheets (Q.1b) on Sheet 6) we considered the squares modulo $p = 19$ (only the numbers $1 \le x \le (p-1)/2 = 9$ needed to be considered, as $(p-x)^2 \equiv x^2 \pmod p$). In fact, we found that all 9 gave different squares. This is true more generally—for this we introduce a notation:

Definition. Let p be a prime and b a number coprime to p. Then we call b a *quadratic residue modulo* p, short *QR* if there is some $x \in \mathbb{Z}$ such that $x^2 \equiv b \pmod p$; otherwise we call b *quadratic non-residue modulo* p, short *NR*.

Example. Writing out the squares modulo 5, we see that $1^2 = 1$, $2^2 = 4$, $3^2 \equiv 4$, $4^2 \equiv 1 \pmod 5$. Hence 1 and 4 are quadratic residues modulo 5, but 2 and 3 are not. ⟦More examples... How to test? Brute force: check all, not efficient, let alone elegant.⟧

Proposition. For an odd prime p, there are precisely $(p-1)/2$ quadratic residues modulo p, and the same number of quadratic non-residues.

Proof: With the above argument we see that there are *at most* $(p-1)/2$ QRs. Now suppose there are two numbers $1 \leq b_1, b_2 \leq (p-1)/2$ with the same squares mod p, i.e. such that $b_1^2 \equiv b_2^2 \pmod{p}$. Then p divides $b_1^2 - b_2^2 = (b_1 - b_2)(b_1 + b_2)$, hence (as p is prime) one of the two factors. It cannot divide the sum, since $1 < b_1 + b_2 \leq p - 1$, which is clearly coprime to p, so it has to divide the difference $b_1 - b_2$, the modulus of which is $< (p-1)/2$, and the only such number divisible by p is 0, hence $b_1 = b_2$.
Conclusion: All these squares are different modulo p, so indeed we get $(p-1)/2$ QRs. Moreover, any other class modulo p except 0 is an NR, hence there are also $(p-1)/2$ many. □

Note. The product of two QRs is again a QR.
⟦If $x \equiv b_1^2$ and $y \equiv b_2^2$, then $xy = (b_1 b_2)^2$.⟧

Slightly more involved is the

Lemma: The product of a QR with an NR is again an NR.
⟦Suppose, for a QR $x = b^2$ and an NR y, the congruence $xy \equiv z$ holds with $z = c^2$ a QR, then multiplying with $x^{-1} \pmod{p}$ (which exists since x as a QR is coprime to p) on both sides would give $y \equiv zx^{-1} \equiv (cb^{-1})^2 \pmod{p}$, a QR; contradiction.⟧

Somewhat surprising, though, might be the following

Lemma: The product of an NR with an NR is a QR.
⟦By multiplying a fixed NR x with all $(p-1)/2$ different QRs we obtain $(p-1)/2$ *different* NRs (use previous lemma and cancellation in $\mathbb{Z}/p\mathbb{Z}$). But this exhausts all the NRs, hence multiplying x with any NR must be a residue mod p different from those NRs, hence a QR. (Why can it not be zero?)⟧

Summarising, we get
Proposition.

$$\begin{aligned} QR \times QR &= QR\,, \\ QR \times NR &= NR\,, \\ NR \times NR &= QR\,. \end{aligned}$$

Those equations should somehow look familiar: replace "QR" by "+1" and "NR" by "−1"...

(9.12.11)

Our calculus with QR and NR motivates the following

Definition/Notation. The *Legendre symbol* of $a \in \mathbb{Z}$ modulo the prime p (for $\gcd(a,p) = 1$) is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is QR}\,, \\ -1 & \text{if } a \text{ is NR}\,. \end{cases}$$

The Legendre symbol is (strictly) multiplicative. In fact, we find

Proposition. Let a, b be integers coprime to the odd prime p. Then we have

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)\,.$$

⟦Proof: immediate from previous proposition (calculus for QR and NR).⟧

Example. For $p = 11$ and $a = 3$ we find

$$\left(\frac{3}{11}\right) = 1\,,$$

since $3 \equiv 25 \pmod{11}$ and 25 obviously *is* a square.

Note: A simple property of the Legendre symbol is that it only depends on the residue of a mod p:

$$\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right) = \cdots = \left(\frac{a+kp}{p}\right)\,, \qquad (k \in \mathbb{Z}).$$

Example 1. The multiplicativity allows us, in a number of cases, to compute rather easily (even by hand) whether a number is a square modulo a prime.
For example, consider the prime $p = 139$ and try to find whether $a = 45$ is a square modulo p. We find

$$\left(\frac{45}{139}\right) = \left(\frac{5 \cdot 3^2}{139}\right) = \left(\frac{5}{139}\right)\left(\frac{3^2}{139}\right)\,.$$

Now due to the fact that $\left(\frac{3^2}{139}\right) = 1$ for obvious reasons (3^2 is not just a QR *modulo* p, but in fact *itself* a square) we can write the above as

$$\left(\frac{5}{139}\right)$$

and since $5 \equiv 144 \pmod{139}$ we can conclude that the latter is $= +1$, and hence indeed that 45 is a square modulo 139.

Note that we *need not* find a square root modulo 139. ⟦In this case it would be provided, e.g., by 36.⟧

Example 2. It may not always be wise to reduce using multiplicativity: what is $\left(\frac{54}{101}\right)$? In this case, it turns out that it is better not to use that $54 = 6 \cdot 3^2$, thereby trying to reduce to the simpler-looking case $\left(\frac{6}{101}\right)$; instead, we look at $54 + k \cdot 101$ for small k; for $k = 2$ we find $54 \equiv 256 = 16^2 \pmod{101}$, so we conclude

$$\left(\frac{6}{101}\right) \equiv \left(\frac{54}{101}\right) = 1\,.$$

Note that the smallest square $\equiv 6 \pmod{101}$ is $1521 = 39^2$.

So far we have fixed a prime p and checked if some a is a square (i.e. QR) modulo p or not.
What if we "wag the dog" and fix a? We will see an amazing regularity starting with $a = -1$.
Q: For which primes p is $a = -1$ a QR? Try to experiment (in PARI the command for $\left(\frac{a}{p}\right)$ is `kronecker(a,p)`) and find a pattern.

We have the following table for *odd* primes:

p	3	5	7	11	13	17	19	23	29	31	37
is -1 QR or NR mod p?	NR	QR	NR	NR	QR	QR	NR	NR	QR	NR	QR
$\left(\frac{-1}{p}\right)$	-1	1	-1	-1	1	1	-1	-1	1	-1	1
$p \pmod 4$	3	1	3	3	1	1	3	3	1	3	1

This seems to suggest:

Proposition. For an odd prime p, we have

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4\,, \\ -1 & \text{if } p \equiv 3 \pmod 4\,. \end{cases}$$

[We will defer the proof to one for a more general statement.]

Note that we also have

$$(-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4\,, \\ -1 & \text{if } p \equiv 3 \pmod 4\,. \end{cases}$$

Hence the proposition implies $(-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right)$.

For a more general statement, we recall that, since $a^{p-1} \equiv 1 \pmod p$, we have (taking square roots mod p) that $a^{(p-1)/2} \equiv \pm 1 \pmod p$.

Theorem. (Euler's criterion) For odd prime p and any $a \in \mathbb{Z}$ coprime to p one has

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p\,.$$

Proof. The idea of the proof is quite simple: for any given primitive root g modulo p the *even* powers g^{2r} $(1 \le r \le (p-1)/2)$, are clearly squares mod p. In fact, they are all different (as g is a primitive root). Hence all the other powers g^{2r-1} $(1 \le r \le (p-1)/2)$ must constitute the other non-zero elements modulo p.
Thus, if a is QR then $a \equiv g^{2r}$ for some r, and

$$a^{(p-1)/2} \equiv g^{2r(p-1)/2} = (g^{(p-1)})^r \equiv 1 \pmod p\,,$$

which is indeed equal to $\left(\frac{a}{p}\right)$.

If, on the other hand, a is NR, then by the above we have $a \equiv g^{2r-1}$ for some r and hence

$$a^{(p-1)/2} \equiv g^{2(r-1)(p-1)/2+(p-1)/2} = (g^{(p-1)})^{r-1} \cdot g^{(p-1)/2} \equiv g^{(p-1)/2} \pmod p\,,$$

and the latter has to be ± 1 (cf. Note above), but cannot be 1, as this would violate that g is primitive mod p. Again, we find that $\left(\frac{a}{p}\right)$ is also -1, hence agrees again with $a^{(p-1)/2} \pmod p$. □

Note that, putting $a = -1$, this also proves our proposition above.

Example. Is -1 QR modulo $p = 2011$?
Since $2011 \equiv 3 \pmod 4$, we have that $(p-1)/2$ is odd, hence conclude that

$$(-1)^{(2011-1)/2} \equiv -1 \pmod{2011}\,,$$

and so -1 is NR modulo 2011.
For the primes $p = 101$ and $p = 641$, we can say that -1 is a quadratic residue mod p.

A much more striking statement arises when we compare the behaviour of two primes relative to each other. For example, we will see that, for primes p and q congruent to 1 (mod 4), one has

$$p \text{ QR } (\text{mod } q) \quad \Leftrightarrow \quad q \text{ QR } (\text{mod } p)\,,$$

or in formulas

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\,.$$

(In fact, this formula will still hold if only one of the two primes is congruent 1 mod p.)

Examples. 1.) Let $p = 13$ and $q = 5$, both congruent to 1 modulo 4.
Since $13 \equiv 3 \pmod 5$, it is an NR mod 5 (QRs are 1 and 4, cf., e.g., last lecture). But it slightly more involved to see that 5 is an NR mod 13 (QRs are ± 1, ± 4, ± 9).

2.) Let $p = 641$ and $q = 13$, both again congruent 1 modulo 4. Then $p \equiv 4 \pmod q$, hence clearly p is a QR mod q. The law above tells us that we also have that q is a QR mod p, and we hence must be able to find a $k \in \mathbb{Z}$ such that $13 + k \cdot 641$ is *a square*. ⟦$k = 3$ does it.⟧

21. Lecture 20 (9.12.11)

We are aiming for the quadratic reciprocity law, and start with a very clever observation by Gauss.

Lemma (Gauss): For an odd prime p and an a coprime to p, consider the set of numbers

$$\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}\,,$$

and reduce them modulo p to numbers in the interval $(-\frac{p}{2}, \frac{p}{2})$.
Then, denoting by ν the number of *negative* numbers in the ensuing set, we have

$$\left(\frac{a}{p}\right) = (-1)^\nu\,.$$

Example: What does the lemma give, say, for $p = 11$ and $a = 3$? The set

$$\{3, 6, 9, 12, 15\}$$

reduces to numbers between $-\frac{11}{2}$ and $\frac{11}{2}$ as

$$\{3, -5, -2, 1, 4\}$$

in which we find 2 negative numbers $-5, -2$, so the lemma gives $\left(\frac{3}{11}\right) = (-1)^2 = 1$, i.e. we expect 3 to be a QR modulo 11 (which is true as $3 \equiv 5^2 \pmod{11}$).

⟦For $a = 7$, we get

$$\{7 \equiv -4, 14 \equiv 3, 21 \equiv -1, 28 \equiv -5, 35 \equiv 3\}$$

for which we find three negative numbers $-4, -1, -5$, hence by the lemma we expect 7 to be a NR modulo 11, which is true as $7 \equiv -4$ and 4 is clearly a QR modulo 11 and -1 is an NR modulo 11 since $11 \equiv 3 \pmod 4$ (cf. last lecture).⟧

For $a = 6$, we get

$$\{6 \equiv -5, 12 \equiv 1, 18 \equiv -4, 24 \equiv 2, 30 \equiv -3\}$$

for which we find three negative numbers $-5, -4, -3$, hence by the lemma we expect 6 to be a NR modulo 11, which is true as $6 \equiv -5$ and $5 \equiv 16$ is a QR modulo 11 and -1 is an NR modulo 11 since $11 \equiv 3 \pmod 4$ (cf. last lecture).

Proof. First observation: of each pair $(1, -1)$, $(2, -2)$, $\ldots$, $(\frac{p-1}{2}, -\frac{p-1}{2})$, at most *one* number appears ⟦otherwise we had two numbers whose sum is divisible by p, which is not possible⟧ and in fact precisely once ⟦otherwise, counting cardinalities of the sets and using the pigeonhole principle, one number would have to appear twice but then the difference would be divisible by p which again is impossible⟧.

Summarising, we find that the set resulting from reducing $S = \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$ to the interval $(-\frac{p}{2}, \frac{p}{2})$ must be of the form

$$T = \{\varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \ldots, \varepsilon_{(p-1)/2} \cdot \frac{p-1}{2}\},$$

with each $\varepsilon_i \in \{\pm 1\}$.
Multiplying together, we find

$$(1a) \cdot (2a) \cdot (3a) \cdots \Big(\frac{p-1}{2}a\Big) \equiv (\varepsilon_1 \cdot 1) \cdot (\varepsilon_2 \cdot 2) \cdots \Big(\varepsilon_{(p-1)/2}\frac{p-1}{2}\Big),$$

and so, after cancellation,

$$a^{(p-1)/2} \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{(p-1)/2} \pmod p.$$

It remains to apply Euler's criterion (cf. previous lecture). □

The following lemma was conjectured by Euler (on the basis of lots of numerical experiments):

Lemma. For an odd prime p and a number $a > 0$ coprime to p one has

(1) The Legendre symbol $\left(\frac{a}{p}\right)$ depends only on p modulo $4a$.
(2) For any prime q with $q \equiv \pm p \pmod{4a}$ one has

$$\Big(\frac{a}{p}\Big) = \Big(\frac{a}{q}\Big).$$

(For a (quite delicate) proof, cf. Stein's book, Prop. 4.3.4.)

The above statements prepare us for one of the jewels in elementary number theory:

Theorem (Quadratic reciprocity law). For any two distinct *odd* primes p, q we have

$$\Big(\frac{p}{q}\Big) = \begin{cases} \Big(\frac{q}{p}\Big) & \text{if } \ p \equiv 1 \pmod 4 \ \text{ or } \ q \equiv 1 \pmod 4, \\ -\Big(\frac{q}{p}\Big) & \text{if } \ p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Another, more succinct way to write this is as follows

$$\textbf{Quadratic reciprocity law:} \qquad \Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Proof. We first deal with the case $p \equiv q \pmod 4$, where, say, $p > q$ and hence $p = q + 4a$ for some $a > 0$. We find

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{4}{a}q\right) = \left(\frac{2}{q}\right)^2\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right)$$

and on the other hand

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right)$$

Now with the previous proposition (conjectured by Euler) we find that $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, as p and q differ by (a multiple of) $4a$.
Therefore, using that $(-1)^{\frac{p-1}{2}}$ is $+1$ for $p \equiv 1 \pmod 4$ and -1 for $p \equiv 3 \pmod 4$, we obtain the statement of the theorem in the two cases $p \equiv q \equiv 1 \pmod 4$ and $p \equiv q \equiv 3 \pmod 4$.
It remains to check the case $p \not\equiv q \pmod 4$, in which case we get $p \equiv -q \pmod 4$. Therefore, in a similar way as above, we find, writing $p = -q + 4a$ for some $a > 0$,

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4a}{q}\right) = \left(\frac{a}{q}\right),$$

and similarly, by symmetry,

$$\left(\frac{q}{p}\right) = \left(\frac{-p+4a}{p}\right) = \left(\frac{a}{p}\right).$$

Again, the previous proposition implies that $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, and so we get indeed

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

which constitutes the remaining claim of the theorem. □

The above reciprocity law allows us to reasonably quickly test whether a number is a square modulo a prime.

Example. Is 17 a square modulo 691?
We compute

$$\left(\frac{17}{691}\right) \overset{\text{Q.R.L.}}{=} \left(\frac{691}{17}\right) = \left(\frac{11}{17}\right) \overset{\text{Q.R.L.}}{=} \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right)$$

which we had seen above to be equal to -1.
Conclusion: 17 is *not* a square modulo 691.

Example. Another example is:

$$\left(\frac{101}{613}\right) = \left(\frac{613}{101}\right) = \left(\frac{7}{101}\right) = \left(\frac{101}{7}\right) = \left(\frac{3}{7}\right) = -1\,.$$

Complement to the Q.R.L.: For an odd prime p, we have

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 8\,, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8\,. \end{cases}$$

A closed formula is

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}\,.$$

Example. -2 is always a QR if $p \equiv 1 \pmod 8$. (e.g. for $p = 89$ get $-2 \equiv 40^2 \pmod{89}$)