Elementary Number Theory and Cryptography, 2014

1 Basic Properties of the Integers $\mathbb{Z}$ and the rationals $\mathbb{Q}$.

Notation. By $\mathbb{Z}$ we denote the set of integer numbers and by $\mathbb{Q}$ we denote the set of rational numbers. We moreover denote the set of positive integer numbers by $\mathbb{N}$. We note that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

Basic Properties:

(1) $(x + y) + z = x + (y + z)$ (*associativity*);

(2) $x + y = y + x$ (*commutativity*);

(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 with respect to addition*);

(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;

(6) $x \cdot y = y \cdot x$;

(7) The equation $a \cdot x = b$ has a unique solution x in $\mathbb{Q}$, provided $a \neq 0$.

(8) $1 \cdot x = x$ (*existence of a neutral element with respect to multiplication*);

(9) $x \cdot (y + z) = x \cdot y + x \cdot z$ (*distributivity*).

We also have an *order relation* in $\mathbb{Z}$ and $\mathbb{Q}$. Every rational (integer) number a is either positive ($a > 0$), negative ($a < 0$) or zero. Then we say that

- $a < b$ if $b - a > 0$; $a \leq b$ if $a < b$ or $a = b$.
- $a > b$ if $b - a < 0$; $a \geq b$ if $a > b$ or $a = b$.

Basic properties of the order relation:

(1) if $x > 0$ and $y > 0$ then $x + y > 0$,

(2) if $x > 0$ and $y > 0$ then $xy > 0$.

(3) $a \leq a$ (*reflexivity*);

(4) If $a \leq b$ and $b \leq a$ then $a = b$ (*antisymmetry*);

(5) If $a \leq b$ and $b \leq c$ then $a \leq c$ (*transitivity*).

Proposition (Principle of the least element). Every nonempty subset of the positive integers contains a smallest element.

Corollary (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 $x \geq 1$.

2 Divisibility.

Definition. Let $a, b \in \mathbb{Z}$. We say that a *divides* b if there exists $x \in \mathbb{Z}$ such that $b = ax$. We will denote it by $a|b$. In the opposite case we write $a \nmid b$ (a does not divide b).

Examples. $-5|30, \quad 17|323, \quad 13|13, \; 13 \nmid 17.$

Properties: For any $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$ we have

- $a|0$;
- $1|c$;
- $a|b$ implies $a|bc$;
- If $a|b$ and $b|c$ then $a|c$;
- If $a|b$ and $a|c$ then $a|bx + cy$ for any $x, y \in \mathbb{Z}$;
- If $a|b$ and $b|a$ then $a = \pm b$;
- If $a|b$ and $a > 0, b > 0$ then $a \leq b$;
- $a|b$ implies $ma|mb$ for any $m \neq 0$.

Example using Mathematical Induction: We prove that for every positive integer n we have $8|5^{2n} + 7$.

We check the base case $n = 1$. We have $5^{2n} + 7 = 5^2 + 7 = 32$ which is indeed divisible by 8. So it holds. We now do the induction step. We assume that we have that 8 divides $5^{2n} + 7$ for all $1, 2, \cdots n$ and we prove it for $n + 1$, that is 8 divides $5^{2(n+1)} + 7$. We use the fact that $a \mid b$ and $a \mid c$ together imply $a \mid b + c$, with $a = 8$, $b = 5^{2n} + 7$ and $c = 5^{2(n+1)} + 7 - (5^{2n} + 7)$. This will then imply the claim as $b + c = 5^{2(n+1)} + 7$. The first divisibility $a \mid b$ is our induction assumption. It remains to show the divisibility for c which can be rewritten $5^{2n}(5^2 - 1)$ and this is clearly divisible by $24 = 5^2 - 1$, which in turn is divisible by 8. By transitivity of divisibility we obtain the claim.

2.1 Division with remainder

Proposition. Let $a \in \mathbb{Z}, b \in \mathbb{N}$. Then there exist *unique* integers q and r such that

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

Then q is called the *quotient* and r is called the *remainder*.

Example: We take $a = 325$ and $b = 17$. Then we have $325 = 19 \cdot 17 + 2$. That is $q = 19$ and $r = 2$.

2.2 The greatest common divisor

Definitions. Let $a, b \in \mathbb{Z}$. A *common divisor* of a and b is any integer d such that $d|a$ and $d|b$. The *greatest common divisor* of a and b is the largest integer g with this property. We denote it by $\gcd(a, b)$:

$$\gcd(a, b) := \max\{d \in \mathbb{Z} \ : \ d|a, d|b\}.$$

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

Basic properties

- $\gcd(a, b) = \gcd(b, a)$;
- If $a \geq 0$ then $\gcd(a, 0) = a$;
- $\gcd(a, b) = \gcd(-a, b)$;
- If $a > 0$ and $b > 0$ then $\gcd(a, b) \leq \min\{a, b\}$.

Examples.

- $\gcd(19, 19) = 19$;
- $\gcd(-15, 25) = 5$;
- $\gcd(42, 30) = 6$;

Lemma. For any integers a, b, q we have

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

Example: We use the lemma to calculate $\gcd(345, 92)$. We have

$$\gcd(345, 92) = \gcd(92, 345) = \gcd(92, 345 - 3 \cdot 92) = \gcd(92, 69) = \gcd(69, 92) =$$

$$\gcd(69, 92-69) = \gcd(69, 23) = \gcd(23, 69) = \gcd(23, 69-3\cdot 23) = \gcd(23, 0) = 23$$

Moreover, working backwards, we have that

$$23 = 92 - 69 = 92 - (345 - 3\cdot 92) = 4\cdot 92 - 1\cdot 345,$$

That is the $\gcd(345, 92)$ can be written as a liner combination of 345 and 92 with integer coefficients.

Euclidean Algorithm. Let a, b be positive integers. The algorithm calculates the $\gcd(a, b)$ as follows: Using division with reminder we find q_i (quotients) and r_i (remainders) in $\mathbb{Z}$ with $0 \leq r_i < r_{i-1}$, $(i = 0, 1, 2, \ldots)$, 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, $r_n = \gcd(a, b)$.

Additionally if in the Euclidean Algorithm we start from the last equality and go up, then we get r_n as the linear combination of a and b:

Corollary. There exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$.

3 Prime and composite numbers

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

Theorem (Euclid) Let p be a prime number and $a, b \in \mathbb{Z}$. If $p|ab$ then either $p|a$ or $p|b$.

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

Fundamental Theorem of Arithmetic (F.T.A). Every positive integer $n > 1$ can be written as a product of primes in a unique way (up to reordering). That is,

$$n = \prod_{j=1}^{m} p_j^{e_j}$$

for some $m, e_j \in \mathbb{N}$ and p_j primes.

Theorem (Euclid) There are infinitely many primes.

Theorem There are infinitely many primes of the form $4n-1$ with $n \in \mathbb{N}$.

Theorem (Dirichlet, without proof) For coprime integers a, b there are infinitely many primes of the form $an+b$ with $n \in \mathbb{N}$.

Euler's Proof of the infiniteness of primes. We now give a sketch of another proof of the infiniteness of primes due to Euler.

For a complex number s with $Re(s) > 1$ we define

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

where n runs over the positive integers. This is the so-called Riemann Zeta Function. It is known that $\zeta(s)$ diverges for $s = 1$.

By using the Fundamental Theorem of Arithmetic we have that $\zeta(s)$ can be written as a product over all the primes (so-called *Euler product*)

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

and the geometric series identity

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

we get

$$\zeta(s) = \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdot \ldots = \prod_p \left(\frac{1}{1-p^{-s}}\right)$$

where the prime is over all prime numbers.

If we now assume that there are only finitely many primes then if we consider the values of $\zeta(s)$ at $s = 1$ we have that the product form $\prod_p \left(\frac{1}{1-p^{-1}}\right)$ is a well defined number. But this contradicts the fact stated above that $\zeta(s)$ diverges for $s = 1$.

The function $\zeta(s)$ encodes information about the distribution of primes. We make this a bit more precise next.

Definition. Let $x \in \mathbb{R}$. By $\pi(x)$ we define the number of prime numbers less or equal to x.

x	10	10^2	10^3	10^4	10^5	10^6	10^7
$\pi(x)$	4	25	168	1229	9592	78498	664579
$\frac{x}{log(x)}$	4.34	21.7	144.7	1085.7	8685	72382	620420

Prime Number Theorem (Hadamard, 1896; without proof):

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

where log denotes the natural logarithm (to base e). In other words we have

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

The proof uses quite deep investigation of the properties of $\zeta(s)$. Actually there is a very famous conjecture (perhaps the most important open conjecture in mathematics today) that is related to the Riemann Zeta Function. Namely,

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

The trivial zeros are the ones of the form $\zeta(-2k) = 0$ for $k = 1, 2, 3, \ldots$. Note that for both the conjecture and the values at negative integers one first have to make sense of the $\zeta(s)$ defined not only for $Re(s) > 1$ but for $s \in \mathbb{C}$. This is possible thanks to the analytic continuation of $\zeta(s)$.

Some more open conjectures with respect to primes:

- There are infinitely many primes of the form $n^2 + 1$.
- There are infinitely many "twin" primes. I. e. the primes p such that $p + 2$ is prime too.
- (Goldbach) Every even number is a sum of two primes.

4 Congruences

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 $n \mid a - b$. Or equivalently we have that $a \equiv b \pmod{n}$ if we write $a = q_1 n + r_1$ with $0 \leq r_1 < n$ $b = q_2 n + r_2$ with $0 \leq r_2 < n$ then $r_1 = r_2$. Sometimes n is called the *modulus*.

Basic properties. For all $a, b, n \in \mathbb{Z}$ and $n \geq 1$ we have:

1. $a \equiv a$ modulo any $n \geq 1$. (Reflexivity)
2. If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$. (Symmetry)
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$. (Transitivity)

These three properties define an equivalence relation. That is we say that two integers are equivalent if they give the same remainder after division by n. In this way we can partition $\mathbb{Z}$ into equivalence classes. Since there are n many possible remainders modulo n we get n many classes.

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 $[a]$. It is called the *residue class* or congruence class modulo n, and a is called a representative of its class.

Example. Let $n = 5$. Then we have the following classes:

$$\begin{array}{lllllll} [0]_5: & -5 & 0 & 5 & 10 & \dots \\ [1]_5: & -4 & 1 & 6 & 11 & \dots \\ [2]_5: & -3 & 2 & 7 & 12 & \dots \\ [3]_5: & -2 & 3 & 8 & 13 & \dots \\ [4]_5: & -1 & 4 & 9 & 14 & \dots \end{array}$$

4.1 Arithmetics modulo n

It appears that for a fixed modulus n we can add, subtract and multiply the classes.

Proposition. Let $n \in \mathbb{Z}, n \geq 1$. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ then

- $a + b \equiv a' + b' \pmod{n}$
- $a \cdot b \equiv a' \cdot b' \pmod{n}$

That is, we can add or multiply classes by picking any representative in the class. Usually the set of classes modulo n is denoted by $\mathbb{Z}/n\mathbb{Z}$. It is a ring (Algebra II).

Example. Take $n = 7$. Then

$$[3] \cdot [5] \equiv [15] \equiv [1] \pmod{7}.$$

If we take another representative of the same class (i.e. [12] instead of [5]) then we have

$$[3] \cdot [12] \equiv [36] \equiv [1] \pmod{7}$$

So the result is the same. If it does not cause the confusion we will omit square brackets and just write

$$3 \cdot 12 \equiv 36 \equiv 1 \pmod{7}$$

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

The proposition shows that in some cases we can even divide out by a class.

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.

A rather canonical choice for a complete set is $R = \{0, 1, \ldots, n-1\}$. However one can choose different complete set. For example the following set is complete set of residues modulo 7

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

Lemma. Let R be a complete set of residues modulo n and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then $aR := \{ax \ : \ x \in R\}$ is also a complete set of residues modulo n.

Definition. A *linear congruence* is an equation in $x \in \mathbb{Z}$ of the form

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

where a, b, and n are given integers ($n \geq 1$).

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

We can solve linear congruences quite efficiently by using the Euclidean algorithm. Indeed if we find $u, v \in \mathbb{Z}$ such that $1 = gcd(a, n) = ua + vn$ then we can take $x = ub$. Indeed we can check that

$$aub \equiv aub + bvn \equiv b(au + vn) \equiv b \cdot 1 \equiv 1 \pmod{n}.$$

We have even the more general proposition:

Proposition. (Without proof) A linear congruence $ax \equiv b \pmod{n}$ is solvable if and only if $\gcd(a, n) \mid b$.

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

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

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

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

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

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

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

We now turn to the computation of $\phi(n)$ for a given $n \in \mathbb{N}$. We have

Lemma. For prime p and positive integer n we have

$$\phi(p^n) = p^n - p^{n-1}.$$

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

$$f(mn) = f(m)f(n)\,. \tag{1}$$

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

Examples.

1. $f(n) = n^k$ for $k \in \mathbb{N}$ is completely multiplicative.
2. The "number of divisors" function $\tau(n) = \sum_{0<d|n} 1$ is multiplicative, but not completely multiplicative. The same holds for the "sum of divisors" function $\sigma(n) = \sum_{0<d|n} d$.

Proposition. Euler's totient function is multiplicative.

The proof of this uses the Chinese Remainder Theorem. This is,

Chinese Remainder Theorem (CRT) Let $n_i \in \mathbb{N}$ for $j = 1, \ldots, r$ with $gcd(n_i, n_j) = 1$ for $i \neq j$. We consider the system of linear congruences

$$x \equiv a_i \pmod{n_i}, \quad i = 1, \ldots r,$$

with $a_i \in \mathbb{Z}$. Then this system of linear congruences has a solution in $x \in \mathbb{Z}$ which is unique modulo $n := \prod_{i=1}^{r} n_i$.

Now we are ready to give a formula for the function $\phi(n)$ if the prime factorization of n is given.

Theorem. Let

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

be a prime factorization of n with $p_i \neq p_j$ for $i \neq j$. Then

$$\phi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Example. $\phi(100) = \phi(2^2 \cdot 5^2) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$.

5 Primality checking

We have two necessary and sufficient conditions for a number n to be a prime. Namely

Theorem. A natural number n is prime if and only if $\forall a \not\equiv 0 \pmod{n}$ one has

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

The condition $a \not\equiv 0 \pmod{n}$ is not equivalent to the condition $gcd(a, n) = 1$ if n is not a prime. We may ask whether we could use in the above theorem the condition $gcd(a, n) = 1$. However the theorem would d no longer be true. Actually we call a composite integer a *Carmichael numbers* if,

$$a^{n-1} \equiv 1 \pmod{n}$$

for all integers a with $gcd(a, n) = 1$. The smallest such number is $n = 561$. Some more are 1105, 1729, 2465, 2821, 6601. Actually it is known that there exist infinitely many of them. Another criterion for primes is the following theorem.

Wilson Theorem. An integer number n is prime if and only if

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

6 Fast exponentiation modulo n (method of successive squaring)

The algorithm for computing $a^m \pmod{n}$:

1. Take the binary expansion of m:
$$m = \epsilon_k 2^k + \epsilon_{k-1} 2^{k-1} + \ldots + \epsilon_1 \cdot 2 + \epsilon_0, \quad \text{with } \epsilon_i \in \{0, 1\}.$$
2. Compute the powers $a^{2^l} \pmod{n}$ for $1 \leq l \leq k$. It will require k modular multiplications. (Next power $a^{2^{l+1}}$ is a square of the previous one a^{2^l}).
3. Finally a^m is the product of those powers a^{2^l} for which the coefficient ϵ_l above equals 1. This will require at most k additional modular multiplications.

The number of modular multiplications in the algorithm is between $\log_2(m)$ and $2\log_2(m)$. So it is very fast. It can be applied for very huge numbers a, m, n.

7 Computing k^{th} roots modulo n

Given $n > 1$, let r be coprime to n, and let k be coprime to $\varphi(n)$. Then a solution of the congruence $x^k \equiv r \pmod{n}$ can be found as follows.

1. Compute $\varphi(n)$.
2. Find an integer a with $0 \leq a < \phi(n)$ and such that $ak \equiv 1 \pmod{\phi(n)}$. That is we find the inverse of k modulo $\phi(n)$. This can be done using the Euclidean algorithm.
3. Then the integer $r^a \pmod{m}$ is a solution. This can be computed using the method of successive squaring described above.

8 Primitive roots

Definition. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. The *multiplicative order* of a modulo n is the smallest positive integer d such that

$$a^d \equiv 1 \pmod{n}.$$

We usually denote it by $\mathrm{ord}_n(a)$. This is well defined since by Euler's Theorem we have $a^{\varphi(n)} \equiv 1 \pmod{n}$, hence we have $ord_n(a) \leq \phi(n)$. Actually we have something stronger, namely

Proposition. $\mathrm{ord}_n(a) | \varphi(n)$.

Definition. An a as above is called (i.e. with $\gcd(a, n) = 1$) is called a primitive root modulo n if $\mathrm{ord}_n(a) = \varphi(n)$.

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 $2^3 \equiv 1$. However there is another primitive root modulo 7, namely 5.

We address the following four questions:

1. Given a prime number p, is there always a primitive root modulo p?
2. If the answer to the above question is yes, then how many are there?
3. Assuming that the answer to the first question again is yes, how to we find a primitive root modulo p?
4. What about general n (not necessarily a prime), is there always a primitive root modulo n?

Theorem. For a prime p and a divisor d of $\varphi(p) = p - 1$, the equation

$$x^d - 1 \equiv 0 \pmod{p}$$

has d incongruent solutions modulo p.

Theorem. For every prime p there exist exactly $\varphi(p-1)$ incongruent primitive roots a modulo p. In particular there always exists at least one primitive root modulo p.

Theorem(Gauss). A primitive root modulo n exists if and only if $n = 2, 4, p^k$ or $2p^k$ where $k \in \mathbb{N}$ and p is an odd prime number.

Important property. Let p be prime and g be a primitive root modulo p. Then every element a with $\gcd(a, p) = 1$ can be written as $a \equiv g^d \pmod{p}$ for some natural d. If we insist that $0 \leq d \leq p - 2$ then this d is unique (depends of course on

g).

Finding primitive roots: There is no efficient way for finding primitive roots modulo a given prime p. The following algorithm relies on the fact that the ratio $\frac{\varphi(p-1)}{p-1}$ is usually quite close to one.

Algorithm.

1. Pick an $a \in \mathbb{Z}$ with $1 \leq a \leq p-1$.
2. Find all different prime divisors of $p-1$, say $p_1, p_2, \ldots, p_r$.
3. Check all the congruences

$$a^{\frac{p-1}{p_k}} \equiv 1 \pmod{p}, \quad 1 \leq k \leq r.$$

   If one of them is satisfied then a is not the primitive root modulo p, and we repeat the algorithm. Otherwise a is a primitive root modulo p.

We mention also an open question.

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

For example, 2 is primitive root modulo $p = 3, 5, 11, 13, 19, 29, \ldots$ but not primitive root modulo $p = 7, 17, 23, 31, \ldots$.

9 Indices and the Discrete Logarithm Problem (DLP)

Let g be a primitive root modulo a prime p. The we have the following crucial property: For any $a \in \mathbb{Z}$, $1 \leq a \leq p-1$ there is precisely one positive integer r with $0 \leq r \leq p-2$ such that $g^r \equiv a \pmod{p}$. In other words the following sets coincide:

$$\{g^0 \pmod{p},\ g^1 \pmod{p}, \ldots,\ q^{p-2} \pmod{p}\} = \{1, 2, \ldots, p-1\}.$$

Definition. Given p and a a primitive root g modulo p, and an $a \in \mathbb{Z}$, $1 \leq a \leq p-1$, we call r as above (i.e. $a \equiv g^r \pmod{p}$) the *index of a modulo p for the base g*. The notation for the index is $I(a) := I_{p,g}(a) = r$. Note that it depends on both p and g.

Example. Take $p = 11, g = 6$

a	1	2	3	4	5	6	7	8	9	10
$I_{11,6}(a)$	0	9	2	8	6	1	3	7	4	5

For a chosen p and g we have:

Proposition. For $a, b, k \in \mathbb{Z}$ with $\gcd(a, p) = \gcd(b, p) = 1$ we have

- $I(ab) = I(a) + I(b) \pmod{p-1}$ (product rule);
- $I(a^k) = k \cdot I(a) \pmod{p-1}$ (power rule).

Knowing the indices for some chosen base g can be very helpful in solving problems which we encounter before. For example,

- **Example 1.** Solve the congruence

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

$$I(x) = I(8^{103}) = 103 \cdot I(8) \equiv 1 \pmod{10}$$

therefore

$$8^{103} \equiv 6^{I(8^{103})} \equiv 6 \pmod{11}.$$

- **Example 2.** Solve the following congruence

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

By passing to indices it gives

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

which leads to the linear congruence

$$3I(x) \equiv 3 \pmod{10} \quad \Rightarrow \quad x \equiv 6 \pmod{11}.$$

The Discrete Logarithm Problem (DLP): Given a prime p, a primitive root g modulo p and a number $1 \leq a \leq p-1$, find $I_{p,g}(a)$. Or equivalently solve the following equation:

$$g^x \equiv a \pmod{p}.$$

There are no known efficient methods which solve the Discrete Logarithm Problem for a general large prime. The (publicly known) record of computing discrete logarithm is for 160-digit prime. m.

10 Applications to Cryptography

Two parties (A (Alice) and B (Bob), say) want to establish a secret key. However they only have the non-secure communication channel which can be intercepted by eavesdropper (E) (Eve).

Even though Alice and Bob want to exchange text messages, they need first to get a number out of it. Assume for simplicity that Alice and Bob exchange messages consisting of only English capital letters i.e. A,B,C...

We start by fixing a bijection between the letters A, B, C, ..., Z of the alphabet and the numbers 1, 2,..., 26. Also add a blank and identify with 0. Then one can transform any message into a number by working with base 27. The key point is that this correspondence has to be one-to-one. Each word corresponds to a unique integer. Here is an example:

Example. Let's turn the word "DURHAM" into the corresponding integer. 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.

So, Alice and Bob want to exchange a number X over the non-secure channel. Traditionally (Symmetric Key Cryptography) this can happen if Alice and Bob shared a secret key K. For practical applications it is desirable to be able to establish this over a non-secure channel.

10.1 Diffie-Hellman Key Exchange

In 1976 Diffie and Hellman suggested the following solution for this problem

1. A and B decide (publicly) on a large (200 digits is usually enough) prime number p and a primitive root g modulo p.

2. A chooses a *secret* random integer m with $1 \leq m \leq p-2$.
   B chooses a *secret* random integer n with $1 \leq n \leq p-2$.

3. A sends $g^m \pmod p$ to B.
   B sends $g^n \pmod p$ to A.

4. Both can now calculate the shared *secret* key given by $K := g^{mn} \pmod p$.

The information available to E is $p, g, g^m \pmod p$ and $g^n \pmod p$. The only known way of calculating $g^{nm} \pmod p$ from that information is to solve DLP problem which is believed to be computationally very hard to solve efficiently.

Example. Take $p = 11$ and $g = 2$ (not real life numbers).

Now Alice chooses (randomly) their secret $m = 6$, hence sends $g^m = 2^6 \equiv 9 \pmod{11}$ to Bob.
Similarly, Bob chooses (randomly) their secret $n = 7$, hence sends $g^n = 2^7 \equiv 7 \pmod{11}$ to Alice.

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

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

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

$$9^7 \equiv 4 \pmod{11}\,.$$

10.2 Public Key Cryptography, RSA

In Public Key Cryptography, opposite to the classical setting, Alice and Bob want to communicate over the non-secure channel *without* sharing a secret key. RSA (Rivest, Shamir, Adleman, 1977) serves this purpose:

Let us assume that Alice wants to send a message, say an integer X, to Bob.
Creation of a Public and a Secret Key (Bob).

1. Choose two different large primes p and q (say, 100 digits long each) and take $n = pq$.
2. Choose a positive number $e < \varphi(n)$ which is coprime to $\varphi(n)$.
3. Find a positive integer d such that $ed \equiv 1 \pmod{\varphi(n)}$.
4. The pair (n, e) is made public. It is called the *public key*. The integer d is called the *private or secret key*. It is kept of course secret.

Encryption (Alice). Given an integer X, the encrypted message is $C := X^e \pmod{n}$. Note that to encrypt the message one just needs to know the public key (n, e).

Decryption (Bob). To decrypt the message C one calculates $C^d \pmod{n}$. This is congruent to X i.e. $X \equiv C^d \pmod{n}$.

The information available to Eve is the public key (n, e) and C. In order to find X she needs to solve the congruence

$$X^e \equiv C \pmod{n}.$$

The only known way of doing that (in general) needs calculation $\varphi(n)$. The following proposition implies that given n, finding $\varphi(n)$ is a shard as factoring n. The last is believed to be a very hard computational problem.

Proposition: Given n (of the form $n = pq, p \neq q$) and $\varphi(n)$, the p, q are the roots of the quadratic equation

$$x^2 - (n - \varphi(n) + 1)x + n = 0$$

.

10.3 Fermat factorization method

In RSA we need to make sure that the number $|p - q|$ is large, that is p and q are not very close. The reason being the following factorization method due to Fermat. Here an n of the form pq is given and the task is to find p and q.

ALGORITHM.

1. Check that n is odd (otherwise the factorization can be easily found).
2. Take $x = \lceil \sqrt{n} \rceil$;
3. Calculate $y = \sqrt{x^2 - n}$;
4. Check if y is an integer. If it is then the required factorization is
$$n = (x - y) \cdot (x + y).$$
5. Otherwise increase x by one and go to step 3.

Example. Take $n = 1692209$. Then $t = 1301$. By applying the algorithm above we find that after fifth iteration we get
$$1692209 = (1301 + 4)^2 - 104^2$$
which then gives the factorization $1692209 = 1201 \cdot 1409$.

10.4 Factoring an RSA modulus "with high probability"

The following algorithm demonstrates that the task of finding d is a shard as factoring n "with high probability".

1. Calculate $m = ed - 1$.
2. Pick a ranom a which is coprime to n and 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 $\not\equiv 1 \pmod n$.
3. If this does not occur for any k for which $m/2^k$ is an integer, go back to step 2 and pick another a.
4. Calculate $gcd(a^{\frac{m}{2^k}} - 1, n)$. If this is not 1 or n then we found a factor of n. Otherwise go back to step 2 and pick another a.

There is a good chance that we will pick an a that satisfies, for $m' = m/2^k$,
$$a^{m'} \equiv \pm 1 \pmod p, \quad a^{m'} \equiv \mp 1 \pmod q,$$
In this case $\gcd(a^{m'} - 1, n)$ will give us a nontrivial divisor of n.

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 $\gcd(a^{3825} - 1, n) = 101$. Therefore we can easily derive that $n = 101 \cdot 103$.

11 Quadratic residues

Definition. Let p be a prime and $a \in \mathbb{Z}$ with $gcd(a,p) = 1$. We call a a *quadratic residue modulo p, QR* if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv b \pmod{p}$; otherwise we call *a quadratic non-residue modulo p, NR.*

Example. We take $p = 7$. Then we have $1^1 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 2$, $5^2 \equiv 4$ and $6^2 \equiv 1 \pmod{7}$. In particular 1,2,4 are QR and 3, 5, 6 are NR.

Proposition. For an odd prime p, there exist exactly $\frac{p-1}{2}$ quadratic residues modulo p, and exactly $\frac{p-1}{2}$ quadratic non-residues modulo p. Note that 0 is not neither a quadratic residue nor a quadratic non-residue. number of quadratic non-residues.

Proposition. The products of the quadratic residues and quadratic non-residues satisfy the following rules:

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

11.1 The Legendre Symbol

Definition. The *Legendre symbol* of $a \in \mathbb{Z}$ modulo the prime p is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is QR}, \\ -1 & \text{if } a \text{ is NR}, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Basic properties of Legendre symbols.

1. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, with $a, b \in \mathbb{Z}$,
2. $\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right), \qquad (k \in \mathbb{Z})$.
3. $\left(\frac{a^2}{p}\right) = 1$ if $gcd(a,p) = 1$.

Examples.

1. $\left(\frac{3}{11}\right) = \left(\frac{3+2\cdot 11}{11}\right) = \left(\frac{25}{11}\right) = \left(\frac{5^2}{11}\right) = 1$,
2. $\left(\frac{45}{139}\right) = \left(\frac{5\cdot 3^2}{139}\right) = \left(\frac{5}{139}\right)\left(\frac{3^2}{139}\right) = \left(\frac{5}{139}\right) = \left(\frac{5+139}{139}\right) = \left(\frac{144}{139}\right) = \left(\frac{12^2}{139}\right) = 1$.

Question. Given a prime p and an $a \in \mathbb{Z}$, how do we calculate $\left(\frac{3}{11}\right)$?

Of course the naive approach is to calculate all $x^2 \pmod p$ for x running over all $x \pmod p$ and see whether a shows up as a square. There are however much more efficient methods.

Theorem. (Euler's criterion) For odd prime p and any $a \in \mathbb{Z}$ with $gcd(a,p)1$ we have,

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

Corollary.

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

Gauss' Lemma. For an odd prime p and an $a \in \mathbb{Z}$ with $gcd(a,p) = 1$, let n denote the number of integers in the set

$$S = \left\{ a, 2a, 3a, \ldots, \frac{p-1}{2}a \right\} ,$$

whose remainder upon division by p exceeds $p/2$, then

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

As the corollary one can deduce the following,

Corollary.

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

The all important theorem due to Gauss is,

Theorem. (Quadratic reciprocity law) Let p, q be two odd primes with $p \neq q$. Then

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

Examples.

1. Compute $\left(\frac{17}{691}\right)$.

$$\left(\frac{17}{691}\right) \overset{\text{Q.R.L.}}{=} \left(\frac{691}{17}\right) = \left(\frac{11}{17}\right) \overset{\text{Q.R.L.}}{=} \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right) \cdot \left(\frac{3}{11}\right).$$

The first term is -1 since $11 \equiv 3 \pmod 8$. For the second one we have

$$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1,$$

since $3 \equiv 3 \pmod 8$. Putting them together we have $\left(\frac{17}{691}\right) = -1$

2.

$$\left(\frac{101}{613}\right) \overset{\text{Q.R.L.}}{=} \left(\frac{613}{101}\right) = \left(\frac{7}{101}\right) \overset{\text{Q.R.L.}}{=} \left(\frac{101}{7}\right) = \left(\frac{3}{7}\right) = -1\,.$$

12 Pythagorean Triples

Definition 1. *A triple* $(x_0, y_0, z_0) \in \mathbb{N}^3$ *is called Pythagorean if*

$$x_0^2 + y_0^2 = z_0^2.$$

Every Pythagorean triple (x_0, y_0, z_0) give rise to an infinite family of Pythagorean triples simply by considering (tx_0, ty_0, tz_0) where $t \in \mathbb{N}$. On the other hand every Pythagorean triple (x_1, y_1, z_1) can be written as (tx_0, ty_0, tz_0) with $gcd(x_0, y_0, z_0) = 1$ and $x_0^2 + y_0^2 = z_0^2$. Pythagorean triples $\gcd(x_0, y_0, z_0) = 1$ are called primitive, as from the observation above it is enough to describe all of them in order to have a description of all Pythagorean triples.

Q. Are there infinitely many primitive Pythagorean triples?

A. Yes. For example one can take triples $(2n^2 + 2n, 2n + 1, 2n^2 + 2n + 1)$ where $n \in \mathbb{N}$.

Q. Are there any other more primitive Pythagorean triples?

A. Yes. For example $(8, 15, 17)$.

Lemma. *In a primitive Pythagorean triple exactly one of* x_0 *or* y_0 *is even and the other is odd.*

Theorem. (x_0, y_0, z_0) *is a Pythagorean triple with even* x_0 *if and only if* $\exists s, t \in \mathbb{N}$ *such that*

- $s > t, \quad s \not\equiv t \pmod 2, \quad \gcd(s, t) = 1$*;*
- $x_0 = 2st, \quad y_0 = s^2 - t^2, \quad z_0 = s^2 + t^2.$

Fermat's Conjecture

About 1637 Fermat stated that $x^n + y^n = z^n,\ n > 2$, has no solutions in integers x, y, z with $xyz \neq 0$. It was proven by A. Wiles in 1995.

Fermat himself proved the case of $n = 4$,

Theorem. *The Diophantine equation*

$$x^4 + y^4 = z^4$$

has no solutions in positive integers x, y, z*.*

This follows from the theorem

Theorem. $x^4 + y^4 = z^2$ *has no solutions in positive integers* x, y, z*.*

Fermat proved this using his Descent Method. The idea is to assume that (x_0, y_0, z_0) is a solution of the equation with z_0 minimal. Then based on this triple we find another solution (x_1, y_1, z_1) with smaller $z_1 < z_0$. But this contradicts to the choice of triple (x_0, y_0, z_0).

Fermat also proved

Theorem. *$x^4 - y^4 = z^2$ has no solutions in positive integers x, y, z.*

The proof of both theorems is based on the idea of *Fermat's infinite descent*:

Sum of Two Squares

We address the question,

Question: Given a positive integer n, can we find two integers a, b such that $n = a^2 + b^2$, or equivalently does the Diophantine equation $n = x^2 + y^2$ have a solution in integers x, y.

Some first few examples,

$$1 = 1^1 + 0^2$$

$$2 = 1^2 + 1^2$$

$$3 \textit{ not possible}$$

$$4 = 2^2 + 0^2$$

$$5 = 2^2 + 1^2$$

$$6 \textit{ not possible}$$

Actually the question can be reduced to the question regarding prime numbers. Indeed by using the equality

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

can be shown easily that

Lemma If $m, n \in \mathbb{N}$ are sum of two squares, so is also their product mn.

As the example with 3 indicated, not all primes can be written as the sum of two squares. Actually we have

Theorem No prime p of the form $4k + 3$ (that is $p \equiv 3 \pmod 4$) can be written as the sum of two squares.

However the situation is different when we consider primes of the form $4k+1$, (that is $p \equiv 1 \pmod 4$). Indeed we have

Theorem An prime of the form $4k+1$ can be written as the sum of two squares.

The key ingredient of the proof of this Theorem is the following Lemma due to Thue.

Lemma Let p be a prime and $a \in \mathbb{Z}$ with $gcd(a,p) = 1$. Then the congruence

$$ax \equiv y \pmod p$$

has a solution x_0, y_0 where

$$0 < |x_0| < \sqrt{p}, \ \ and \ \ 0 < |y_0| < \sqrt{p}.$$

The main idea for the proof of this lemma is the so-called "Pigeon-Hole Principle".

Pigeon-Hole Principle: If n objects are placed in m boxes (or pigeon-holes) and if $n > m$, then some box will contain at least two objects.

Moreover we can also address the question whether one can represent a prime as the sum of two squares in a unique way (not counting change of signs of course).

Proposition Let p be a prime with $p \equiv 1 \pmod 4$. The p can be written in a unique way as the sum of two squares

Going back to the initial question, for any given integer n, we have

Theorem Let $n = N^2 m$ with m square free. Then n can be represented as the sum of two squares if an only if m does not contain any prime factor of the form $4k+3$.

Sum of Three and Four Squares

If we give ourselves more freedom, namely to increase the number of squares in the representation we can obtain "more" integers. Indeed we have.

Theorem Any integer not of the form $4^n \cdot (8m+7)$ with $n, m \in \mathbb{Z}$, and $n, m \geq 0$ can be written as the sum of three squares.

In the lectures we proved the necessary condition (namely that no integer of the form can be written as the sum of three squares), while the other direction is harder, due to the fact that we are lacking an identity to write the product of the sum of three squares as the sum of three squares. Something available in the two squares situation. Moreover we mention without proof the following theorem of Lagrange

Theorem Any integer can be written as the sum of four squares.

Finite Continued Fractions

Definition A *finite continued fraction* is a number of the form

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots\cdots \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}}}$$

where $a_0, a_1, \ldots, a_n \in \mathbb{R}$, all of which except possible a_0 are positive. The numbers $a_0, a_1, \ldots, a_n$ are called the *partial quotients*. The fraction is called *simple* if all the a_i's are integers. Such a number we denote by $[a_0; a_1, a_2, \ldots, a_n]$.

Examples

1. $$[1; 1, 2] = 1 + \frac{1}{1 + \frac{1}{2}} = \frac{5}{3}.$$

2. $$[3; 1, 4, 2] = 3 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2}}} = \frac{42}{11}.$$

Theorem. *Any rational number can be written as a finite simple continued fraction.*

Q. Is this representation unique?

A. Any $\frac{p}{q}$ is uniquely written as $[a_0; a_1, \ldots, a_n]$ with $a_n \geq 2$. However there is always 2-nd possibility with the last partial quotient 1.

$$[a_0; a_1, \ldots, a_n] = [a_0; a_1, \ldots, a_n - 1, 1].$$

Usually the first representation is used. It is called *canonical*.

Definition The k-th convergent, for $0 \leq k \leq n$, of $[a_0; a_1, \ldots, a_n]$ is the number $C_k = [a_0; a_1, \ldots, a_k]$. Here we take $C_0 = a_0$.

We usually write it as the fraction $C_k = \frac{p_k}{q_k}$. It appears that convergents can be calculated quite easily by using the following property.

Theorem. *Convergents can be calculated by the following recurrent formulas.*

$$\begin{array}{lll} p_0 = a_0, & p_1 = a_0 a_1 + 1 & p_k = a_k p_{k-1} + p_{k-2}, \\ q_0 = 1, & q_1 = a_1 & q_k = a_k q_{k-1} + q_{k-2}. \end{array}$$

Example. Consider the number $\alpha = \frac{767}{201} = [3; 1, 4, 2, 3, 5]$. Then the convergents are as follows:

a_k	3	1	4	2	3	5
p_k	3	4	19	42	145	767
q_k	1	1	5	11	38	201

The main properties of the convergents $C_k = \frac{p_k}{q_k}$ of a finite simple continued fraction are

1. $p_k, q_k \in \mathbb{Z}$

2. $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$,

3. $gcd(p_k, q_k) = 1$,

4. $0 < q_0 \leq q_1 < q_k < q_{k+1}$ for $k \geq 2$,

5. $C_0 < C_2 < C_4 < \ldots < C_{2k} < C_{2k+2} < \ldots$,

6. $C_1 > C_3 > C_5 > \ldots > C_{2k+1} > C_{2k+3} > \ldots$,

7. $C_{odd} > C_{even}$

Infinite Continued Fractions

Let $a_0, a_1, a_2, \ldots$ be an infinite collection of integers, all of which, except possibly a_0, are taken to be positive. We define the infinite continued fraction $[a_0; a_1, a_2, \ldots,]$ as the limit of its convergents:

$$[a_0; a_1, a_2, \ldots] := \lim_{n\to\infty} C_n.$$

where $C_n = [a_0; a_1, a_2, \ldots, a_n]$. The existence of the limit can be shown be considering the limits $\alpha^{odd} := \lim_{n\to\infty} C_{2n+1}$ and $\alpha^{even} := \lim_{n\to\infty} C_{2n}$. The first exists because the $\{C_{2n+1}\}$ is a strictly decreasing sequence bounded from below, and $\{C_{2n}\}$ increasing and bounded from above. Since the distance between C_n and C_{n+1} tends to zero as n goes to infinity we have that $\lim_{n\to\infty} C_n$ exists.

A real number x is called irrational if $x \notin \mathbb{Q}$, that is there exist no $a, b \in \mathbb{Z}$ such that $x = \frac{a}{b}$.

Theorem: The value of every infinite continued fraction is an irrational number.

Theorem: For any irrational number x there exists a unique infinite continued fraction such that

$$x = [a_0; a_1, \ldots].$$

Given an irrational number x_0 we can compute its n^{th} partial denominator a_n in its infinite continued fraction representation by using the following algorithm:
We set $a_0 := [x_0]$ and then

$$x_1 := \frac{1}{x_0 - [x_0]}, \quad a_1 := [x_1],$$

$$x_2 := \frac{1}{x_1 - [x_1]}, \quad a_2 := [x_2],$$

$$x_n = \frac{1}{x_{n-1} - [x_{n-1}}, \quad a_n := [x_n]$$

Example. Find the continued fraction for $\sqrt{5}$.

$$\sqrt{5} = 2 + (\sqrt{5} - 2); \quad \frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2 = 4 + (\sqrt{5} - 2);$$

$$\frac{1}{\sqrt{5}-2} = \sqrt{5}+2 = 4+(\sqrt{5}-2); \ldots$$

So $\sqrt{5} = [2; 4, 4, 4, 4, \ldots] = [2, \overline{4}]$.
Infinite continued fractions of the above form are called periodic. That is, we write $[a_0; a_1, \ldots, a_m, \overline{b_1, \ldots b_n}]$ for the infinite continued fraction of the form

$$[a_0; a_1, \ldots, a_m, b_1, \ldots b_n, b_1, \ldots b_n, b_1, \ldots b_n, \ldots]$$

that is the string $b_1, \ldots b_n$ repeats itself. Moreover we say that it of period of length n.
Theorem Let x be an irrational number. Then the infinite continued fraction of x is periodic if and only if x is of the form $r + s\sqrt{d}$ with $r \in \mathbb{Q}$, $0 \neq s \in \mathbb{Q}$ and $d \in \mathbb{N}$ but not a square.

13 Application of infinite continued fraction to the approximation of irrational numbers

Infinite continued fractions, and in particular its convergents, can be used to provide "optimal" approximations of irrational numbers by rational numbers. We list two theorems in this direction.

Theorem If $\frac{p_n}{q_n}$ is the n^{th} convergent of the irrational number x, then

$$|x - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

So we see that the convergent approximate the irrational number with precision measured by the denominator of the convergent. We may ask the question.

Q: Given an irrational number x, how closely can be approximated by rational numbers?

Theorem: Let x be an irrational number. Then

1. If $1 \leq b \leq q_n$, the rational number $\frac{a}{b}$ satisfies

$$|x - \frac{p_n}{q_n}| \leq |x - \frac{a}{b}|.$$

2. If the rational number $\frac{a}{b}$, where $b \geq 1$ and $\gcd(a, b) = 1$ satisfies

$$|x - \frac{a}{b}| < \frac{1}{2b^2}$$

then $\frac{a}{b}$ is a convergent of x.

The above theorem indicates that the convergents of an irrational number x are the best rational approximations to x, in that every other rational number with the same or smaller denominator differs from x by a larger amount.

14 Pell's Equation

Let d be a positive integer, which is not a square. Then Pell's equation is the diophantine equation of the form

$$x^2 - dy^2 = 1.$$

The following theorem describes all positive solutions in x and y of the above equation.

Theorem Let $\frac{p_m}{q_m}$ denote the m^{th} convergent of the infinite continued fraction of $\sqrt{d}$. Let n be the length of the period of the continued fraction expansion of $\sqrt{d}$. Then

1. If n is even, then all positive solutions of $x^2 - dy^2 = 1$ are given by

$$x = p_{kn-1}, \quad y = q_{kn-1}, \quad k = 1, 2, 3, \ldots$$

2. If n is odd, then all positive solutions are given by

$$x = p_{2kn-1}, \quad y = q_{2kn-1}, \quad k = 1, 2, 3, \ldots$$

15 The General Discrete Logarithm Problem

We start by defining some notion form group theory.

Definition: A set G equipped with an operation $*$ (that is for $g_1, g_2 \in G$ we have $g_1 * g_2 \in G$) is called a group if the following hold

1. $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$
2. there exists an $e \in G$, usually called the neutral or identity element such that $g * e = e * g = g$ for all $g \in G$.
3. for all $g \in G$, there exists an element in G, usually denoted by g^{-1} such that $g * g^{-1} = g^{-1} * g = e$. The element g^{-1} is called the inverse of g with respect to the operation $*$.

We usually denote a group by $(G, *)$ when we want to make clear the operation. When this is clear we usually write just G. Finally if for any $g_1, g_2 \in G$ we have $g_1 * g_2 = g_2 * g_1$, then the group is called abelian.

Examples: The following are all abelian groups

1. $(\mathbb{Z}, +)$,
2. $(\mathbb{Z}/n\mathbb{Z}, +)$,
3. $((\mathbb{Z}/n\mathbb{Z})^{\times}, \cdot)$.

We can build groups from another groups. One way to do this is by forming the direct product of two groups. Namely if $(G_1, *_1)$ and $(G_2, *_2)$ are two groups then we may define $(G_3, *_3)$ as follows

$$G_3 = G_1 \times G_2 = \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_2\}$$

and $(g_1, g_2)_3(g_1', g_2') = (g_1 *_1 g_1', g_2 *_2 g_2')$. It is clear that if G_1 and G_2 are both abelian then so is also $(G_3, *_3)$. When operations are clear we usually write $G_1 \times G_2$ for G_3.

Definition Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups. A map $f : G_1 \to G_2$ is called a group homomorphism if $f(g_1 *_1 g_2) = f(g_1) *_2 f(g_2)$ for $g_1, g_2 \in G_1$. A group homomorphism which is bijective is called a group isomorphism and in this case the two groups are called isomorphic.

Definition Let $(G, *)$ be a group. A subset $H \subseteq G$ is called a subgroup of G if H is a group with respect to the operation $*$.

Theorem If G is a finite group and H is a subgroup of G, then if we write $\sharp G$ (resp $\sharp H$) for the order (i.e. number of elements in the set G) of G (resp H), then

$$\sharp H \mid \sharp G,$$

that is the integer $\sharp H$ divides the integer $\sharp G$.

Given a group $(G, *)$, an element $g \in G$ and a positive integer m we define

$$[m]g := g * g * g * \ldots * g,$$

where g appears m-many times. We also define $[0]g = e$ (the identity) and $[-m]g := [m]g^{-1}$. We consider the set

$$< g >:= \{e, [\pm 1]g, [\pm 2]g, [\pm 3]g, \ldots, [\pm m]g, \ldots\}$$

Then $(< g >, *)$ is a subgroup of G, and it is called the subgroup of G generated by the element g.

General Discrete Logarithm Problem Let $(G, *)$ be an abelian group and let $g \in G$ be an element different from e. Given $h \in < g >$ find an $m \in \mathbb{Z}$ such that

$$h = [m]g$$

If we take $(G, *) = ((\mathbb{Z}/p\mathbb{Z})^{\times}, \cdot)$, where p is a prime and g a primitive root modulo p, then the General Discrete Logarithm Problem is the "classical" Discrete Logarithm Problem which we have seen in the Michaelmas Term.

The General Discrete Logarithm Problem may be quite easy for some choices of the group $(G, *)$. For example if we take $(\mathbb{Z}/p\mathbb{Z}, +)$ and g any non-zero element, it can be solved very easily using the Euclidean Algorithm.

16 Elliptic Curves defined over $\mathbb{Q}$

We start with the definition of elliptic curves defined over the rational numbers.

Definition An elliptic curve E, defined over $\mathbb{Q}$ is the set of solutions of the equation

$$Y^2 = X^3 + aX + b,$$

with $a, b \in \mathbb{Z}$, $\Delta := 4a^3 + 27b^2 \neq 0$ and a rational point at infinity $\mathcal{O}$. Δ is often called the discriminant of E.

The high interest in elliptic curves is due to the fact that they posses a group structure. This is defined as follows.

Group Structure: We give to the set $E \cup \{\mathcal{O}\}$ a groups structure, where the operation will be denoted by $\oplus$, as follows,

1. The neutral or identity element is $\mathcal{O}$. That is for any point $P \in E$ we have $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$, $\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$.
2. Given $P = (x, y) \in E$ we define its inverse by $-P = (x, -y)$. Moreover $-\mathcal{O} = \mathcal{O}$
3. Given $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $P_1, P_2 \in E$ we define $P_3 = P_1 \oplus P_2$ as follows
   (a) If $P_1 \neq P_2$ and $x_1 \neq x_2$ then we define $P_3 = (x_3, -y_3)$ where $x_3 := \lambda^2 - x_1 - x_2$, $y_3 := \lambda x_3 + \nu$, $\lambda := \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu := y_1 - \lambda x_1$.
   (b) If $P_1 \neq P_2$ and $x_1 = x_2$, then this implies in particular that $y_1 = -y_2$ and hence we obtain $P_1 \oplus p_2 = \mathcal{O}$.
   (c) If $P_1 = P_2$ and $y_1 \neq 0$ then we define $P_3 = (x_3, -y_3)$ by $x_3 := \lambda^2 - 2x_1$, $y_3 := \lambda x_3 + \nu$, $\lambda := \frac{3x_1^2 + a}{2y_1}$ and $\nu := y_3 - \lambda x_3$.
   (d) If $P_1 = P_2$ and $y_1 = 0$ then we have that $P_1 \oplus P_1 = \mathcal{O}$.

One can check that the above operation is associative (i.e. $P_1 \oplus (P_2 \oplus P_3) = (P_1 \oplus P_2) \oplus P_3$ and the group is abelian, that is $P_1 \oplus p_2 = P_2 \oplus p - 1$.

We define the set

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 | (x, y) \in E\} \cup \{\mathcal{O}\}$$

The set $E(\mathbb{Q}0$ has also the structure of an abelian group. Indeed one can check that $P \oplus Q \in E(\mathbb{Q})$ if $P, Q \in E(\mathbb{Q})$.

Mordell's Theorem: The abelian group $E(\mathbb{Q})$ is finitely generated.

We call a point $P \in E$ a torsion point or point of finite order if there exists an $m \in \mathbb{N}$ such that $[m]P = \mathcal{O}$. The set of the torsion points is a subgroup of E. The set of torsion points of E which are also in $E(\mathbb{Q})$c is denoted by $E(\mathbb{Q})_{tors}$, and it is a

subgroup of $E(\mathbb{Q})$.

Nagell-Lutz Theorem Let E be an elliptic curve defined by $Y^2 = X^3 + aX + b$ with $a, b \in \mathbb{Z}$ and $\Delta = 4a^3 + 27b^2 \neq 0$. Let $\mathcal{O} \neq P = (x, y) \in E(\mathbb{Q})_{tors}$. Then $x, y \in \mathbb{Z}$ and either i) $y = 0$ in which case P is of order two or ii) y^2 divides Δ.

Mazur's Theorem The group $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups

1. $\mathbb{Z}/N\mathbb{Z}$ where $1 \leq N \leq 10$ or $N = 12$,
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, $1 \leq N \leq 4$.

17 Elliptic Curves over finite fields.

Fields: A set K equipped with two operations $+, \cdot$ is called a field if

1. $(K, +)$ is an abelian group with a neutral element 0,
2. $K^\times, \cdot)$ is an abelian group with a neutral element $1 \neq 0$, where $K^\times := K - \{0\}$.
3. For $a, b, c \in K$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$.

The main examples for this course are the field of rational numbers $\mathbb{Q}$ with the usual addition and multiplication, and the set $\mathbb{Z}/p\mathbb{Z}$ for p a prime number with the usual addition and multiplication. The last is usually denoted by $\mathbb{F}_p$ when we want to indicate the field structure.

Definition Let p be an odd prime. An elliptic curve E, defined over $\mathbb{F}_p$ is the set of solutions of the equation

$$Y^2 = X^3 + aX + b,$$

with $a, b \in \mathbb{F}_p$, $\Delta := 4a^3 + 27b^2 \neq 0$ (the last as element in $\mathbb{F}_p$) and an $\mathbb{F}_p$ rational point at infinity $\mathcal{O}$.

Of special interest is for us the set:

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

Using exactly the same definitions as we did over the rational numbers we can make this an abelian group. Of course now all the operations are happening over the field $\mathbb{F}_p$.

Theorem: The group $E(\mathbb{F}_p)$ is isomorphic to either i) $\mathbb{Z}/d_1\mathbb{Z}$ where $d_1 \in \mathbb{N}$ or ii) $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_1d_2\mathbb{Z}$ where $d_1, d_2 \in \mathbb{N}$ with $d_1 \geq 2$.

Hasse's Theorem: For an elliptic curve E defined over the finite field $\mathbb{F}_p$ we have

$$|\sharp E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}.$$

There is a relation between an elliptic curve define over the rational numbers and elliptic curves defined over $\mathbb{F}_p$, where p an odd prime. Indeed if E is an elliptic curve defined by

$$Y^2 = X^3 + aX + b,$$

where $a, b \in \mathbb{Z}$ and $\Delta = 4a^3 + 27b^2 \neq 0$. For any odd prime p that p does not divide Δ then we can use the same equation to define an elliptic curve over the finite field $\mathbb{F}_p$ where we take the integers a, b modulo p. We have:

Theorem (Reduction modulo p): Let E be an elliptic curve defined over $\mathbb{Q}$, and let Δ be its discriminant. Then for any odd prime P which does not divide Δ we have an injective homomorphism

$$E(\mathbb{Q})_{tors} \to E(\mathbb{F}_p),$$

and the map is given by sending $(x, y) \in E(\mathbb{Q})_{tors}$ to $(x \pmod p, y \pmod p) \in E(\mathbb{F}_p)$, and the point at infinity to the point at infinity.

18 Elliptic Curve Cryptography

We can use the theory of elliptic curves for Key Exchange.

Elliptic Curve Key Exchange Protocol:

1. Alice and Bob agree, over the public channel, on an elliptic curve E, defined over a finite field $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$.
2. Alice selects an integer $m \in \mathbb{N}$, and computes the point $Q := [m]P$.
3. Bob selects an integer $n \in \mathbb{N}$, and computes the point $R := [n]P$.
4. Alice sends the point Q to Bob, and Bob sends the point R to Alice.
5. Alice computes $[m]R = [m][n]P = [mn]P$, and Bob computes $[n]Q = [n][m]P = [nm]P$. The common secret key is $K = [mn]P$.

Eve sees E, $\mathbb{F}_p$, P, Q and R. Eve could try to recover m or n by solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) namely $Q = [m]P$ or $R = [n]P$ to recover n or m. This is believed to be computationally hard.

We can use elliptic curves also to implement Public Key Cryptography.

The ElGamal Public Key Cryptography Protocol:

1. Alice and Bob agree, over the public channel, on an elliptic curve E, defined over a finite field $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$.
2. Alice selects an integer a, and computes the point $A := [a]P$. The point A is the public key, and the integer a is the secret key.
3. Bob wants to send the message $M \in E(\mathbb{F}_p)$. He chooses an integer k, and computes $B_1 := [k]P$ and $B_2 = M + [k]A$. He sends $B - 1$ and B_2 to Alice.
4. Alice computes $B_2 - [a]B_1$.

Alice recovers indeed the message M since,

$$B_2 - [a]B_1 = (M + [k]A) - [a][k]P = M + [ka]P - [ka]P = M.$$

Eve sees $E, \mathbb{F}_p, A, B_1, B_2, P$. A way to recover M is to solve the ECDLP $B_1 = [k]P$, or $A = [a]P$.

Elliptic Curve Digital Signature Protocol:

1. Alice and Bob agree, over the public channel, on an elliptic curve E, defined over a finite field $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$ of prime order q.

2. Alice selects an integer a and compuets $A := [a]P$. Alice publishes A (public verification key) and keeps a secret (secret signing key).

3. Let $d \pmod q$ be the digital document. Alice picks an integer $0 \neq k \pmod q$ and computes $[k]P$ and sets

$$s_1 \equiv x([k]P) \pmod q, \quad s_2 \equiv (d + as_1)k^{-1} \pmod q,$$

where $x([k]P) = 0, 1, 2, \ldots, p-1$ the x-coordinate of the point $[k]P$. The signature of Alice for the document d is (s_1, s_2).

4. In order for Bob to verify that indeed the document d was signed by Alice he computes

$$v_1 \equiv ds_2^{-1} \pmod q, \quad v_2 \equiv s_1 s_2^{-1} \pmod q,$$

and verifies whether

$$x([v_1]P + [v_2]A) \equiv s_1 \pmod q.$$

If the last equality holds, then then document d with signature (s_1, s_2) was signed by Alice, otherwise was not. Given d, in order Eve to reproduce the signature s_1, s_2 she has to solve an ECDLP.

19 Some Examples.

1. Consider the curve E defined by the equation

$$Y^2 = X^3 + X + 1.$$

   (a) Show that E is an elliptic curve defined over the field $\mathbb{F}_5$, and determine the group $E(\mathbb{F}_5)$.

   (b) Show that E is an elliptic curve defined over the field $\mathbb{F}_7$ and determine the group $E(\mathbb{F}_7)$.

   Ans.

(a) We compute $\Delta = 4 \cdot 1^3 + 27 \cdot 1^2 \equiv 1 \pmod 5$. Hence $\Delta \neq 0$ in $\mathbb{F}_5$ so E is an elliptic curve defined over $\mathbb{F}_5$. In order to determine $E(\mathbb{F}_5)$ as a set we just check all possible values that Y^2 can take for all possible values of Y in $\mathbb{F}_5$, that is $Y = 0, \pm 1, \pm 2$ and similarly for $X^2 + X + 1$ where $X = 0, \pm 1, \pm 2$. Then we see that the set of points is given by (always we have the point at infinity)

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0, \pm 1), (2, \pm 1), (-2, \pm 1), (-1, \pm 2)\}$$

So we have that the cardinality of $E(\mathbb{F}_5)$ is 9. In order to determine the group structure of this set we recall from the lectures that $E(\mathbb{F}_5)$ is either of the form $\mathbb{Z}/d\mathbb{Z}$ for $d \in \mathbb{N}$ or $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_1 d_2\mathbb{Z}$ for $d_1, d_2 \in \mathbb{N}$ and $d_1 \geq 2$. That means that $E(\mathbb{F}_5)$ is either isomorphic to $\mathbb{Z}/9\mathbb{Z}$ or to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. In order to determine which group $E(\mathbb{F}_5)$ it is enough to check whether $E(\mathbb{F}_5)$ has any point of order larger than 3 since all the elements in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ have order at most three (check!). We take $P = (0, 1)$. Then we compute using the method from above that $[2]P = (-1, 2)$ and $[3]P = P \oplus [2]P = (2, 1)$. In particular $[3]P \neq \mathcal{O}$ and hence P has order larger than 3. That is $E(\mathbb{F}_5)$ is isomorphic to $\mathbb{Z}/9\mathbb{Z}$, and actually we have also seen that $E(\mathbb{F}_5) =< P >$.

(b) We have $\Delta = 31 \equiv 3 \pmod 7$. That is $\Delta \neq 0$ in $\mathbb{F}_7$ and hence E is an elliptic curve over $\mathbb{F}_7$. As above by doing an exhaustive search of all possible points we find that the set $E(\mathbb{F}_7)$ is given by

$$E(\mathbb{F}_7) = \{\mathcal{O}, (0, \pm 1), (2, \pm 2)\}.$$

That is $E(\mathbb{F}_7)$ is of size 5. The only possibility is then (since 5 is a prime) that $E(\mathbb{F}_5)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. We moreover note that for any point $P \in E(\mathbb{F}_7)$ different to $\mathcal{O}$ we have $E(\mathbb{F}_7) =< P >$.

2. Consider the curve E defined by the equation

$$Y^2 = X^3 + 2X + 1.$$

Show that E is an elliptic curve defined over the field $\mathbb{F}_5$, and determine the group $E(\mathbb{F}_5)$.

Ans. We compute $\Delta = 4 \cdot 2^3 + 27 \cdot 1^2 = 32 + 27 = 59 \equiv 4 \neq 0 \pmod 5$. Hence E is an elliptic curve over $\mathbb{F}_5$. The set $E(\mathbb{F}_5)$ is given by

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0, \pm 1), (1, \pm 2), (-2, \pm 2)\}.$$

In particular it is of size 7. Hence it has to be isomorphic to $\mathbb{Z}/7\mathbb{Z}$.

3. Consider the curve E defined by the equation

$$Y^2 = X^3 + 6X + 1.$$

Show that E is an elliptic curve defined over the field $\mathbb{F}_7$, and determine the group $E(\mathbb{F}_7)$.

Ans. We first note that since we are working over $\mathbb{F}_7$ the above equation is equivalent to the equation

$$Y^2 = X^3 - X + 1$$

We compute now $\Delta = 4 \cdot (-1)^2 + 27 \cdot 1^3 = 31 \equiv 3 \neq 0 \pmod 7$. Hence E is an elliptic curve. Computing the set $E(\mathbb{F}_7)$ we find that

$$E(\mathbb{F}_7) = \{\mathcal{O}, (0, \pm 1), (1, \pm 1), (2, 0), (3, \pm 2), (-2, \pm 3), (-1, \pm 1)\}.$$

Hence $E(\mathbb{F}_7)$ is of size 12. Hence the possibilities are $\mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. In order to distinguish between the two groups we calculate the orders of some of the points of $E(\mathbb{F}_7)$. We take $P = (0, 1)$. Then we compute that (check) $[2]P = (2, 0)$ Hence $[2]P$ is a point of order 2, which makes P a point of order 4, and hence the same holds for $-P = (0, -1)$. Now we check the point $Q = (-2, 3)$. We have $[2]Q = (-1, 1)$ and moreover $[4]Q = [2]Q \oplus [2]Q = (3, -2) \neq \mathcal{O}$. Since $(3, -2)$ is not of order two (why?) we can conclude that Q is of order 12, since we have that Q has order larger than 6, and the size of $< Q >$ has to divide 12. In particular $E(\mathbb{F}_7)$ has a point of order 12, and hence cannot be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Hence it is isomorphic to $\mathbb{Z}/12\mathbb{Z}$.