ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY II
SOLUTIONS OF PROBLEM SHEET 2
MICHAELMAS TERM 2014

(1) We want to choose n to have a nontrivial gcd with each of $n+2$, $n+3$, ..., $n+k$. Noting that $\gcd(n, n+j) = \gcd(n, j)$ for any $j \in \mathbb{Z}$ we can assure this by simply demanding that $\gcd(n, j) = j$ for $j = 2, \ldots, k$. A natural candidate is $n = 2 \cdot 3 \cdots k$, i.e. $n = k!$.
But we can in fact take n to be the product $m \cdot (m+1) \cdots (m+k)$ of any k successive positive integers, keeping in mind that the binomial coefficient $\binom{m+k}{k} = \frac{m \cdot (m+1) \cdots (m+k)}{1 \cdot 2 \cdots k}$ for $m \geq 0$ is an integer, hence $k!$ divides such a product.

(2) By the fundamental theorem of arithmetic a can be written as $a = p_1 \cdot p_2 \cdot \ldots p_n$ for some prime numbers p_i, and $n \geq 2$. Assume witout loss of generality that $p_1 \leq p_i$ for all i. Then we have that $a \geq p_1^n \geq p_1^2$. Hence $p_1 \leq \sqrt{a}$.

(3) Denote the ten consecutive numbers n, $n+1$, ..., $n+9$.
• We note that $g := \gcd(n+j, n+k) = \gcd(n+j, k-j) \leq |k-j| \leq 9$, so if $g > 1$ then it must be divisible by one of the four primes 2, 3, 5 or 7, and hence the same is true for $n+j$ (and $n+k$).
• But there are at most nine numbers among those 10 which are divisible by any of these 4 primes ⟦there are precisely 5 even ones, which we can immediately discard, and among the 5 remaining *odd* ones there are at most two which are divisible by 3 and at most 1 each divisible by 5 or 7⟧, so at least one of the $n+j$ has gcd not divisible by any of the four primes, hence by the above must have a gcd equal to 1 with *each* of the other nine.
• Now use e.g. that $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ implies that $\gcd(a, bc) = 1$ (why?) to conclude that this $n + j$ has gcd equal to 1 with the product of the other nine.

(4) Suppose $\sqrt{p} \in \mathbb{Q}$. Then there exist $a, b \in \mathbb{Z}$ with $gcd(a, b) = 1$ such that $\sqrt{p} = \frac{a}{b}$. Taking squares we get $b^2 = pa^2$. We now claim that $b = 1$. Assume that $b > 1$, and let q be a prime that divides b. Since $b|b^2$ and $b^2 > a^2$ we have that $q|a^2$, and since q is a prime we have that $q|a$. But then we have that $gcd(a, b) \geq q$. Contradiction. Hence we have $b = 1$. But then we have that $p = a^2$. But p is a prime hence we again derive a contradiction.

(5) (a) We consider the number $N := p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. As in Euclid's proof we have that none of the p_i's divides N. By F.T.A. we have that there exists q prime such that $q|N$. Hence we have that $q > p_n$. In particular $q \geq p_{n+1}$. On the other hand since q divides N we have that $q \leq N$. Hence we conclude that $p_{n+1} \leq p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

(b) We rewrite the statement as $p_n \leq 2^{2^{n-1}}$ and do induction on n. For $n = 1$ it is clear true since $2 \leq 2$. We assume that it is true for all integers up to n and prove it for $n + 1$. We have by the previous

question and the induction assumption

$$p_{n+1} \leq p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \leq 2 \cdot 2^2 \cdot 2^3 \ldots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\ldots+2^{n-1}} + 1 = 2^{2^n-1} + 1.$$

But $1 \leq 2^{2^{n-1}}$ for all $n \geq 1$ and hence we have that $p_{n+1} \leq 2 \cdot 2^{2^n-1} = 2^{2^n}$.

(c) From the previous question we know that $p_{n+1} \leq 2^{2^n}$. Hence p_1, p_2 up to p_{n+1} are less than 2^{2^n} (Note that the statement is true for $n = 1$ and for any $n > 1$ we have that $p_{n+1} < 2^{2^n}$ since it is odd.

(6) (a) The numbers of the form $3n+1$ have either the form $6n+1$ or $6n+4$; but the latter ones are always even and > 2, hence can never be prime.

(b) Show that the product of two integers of the form $3n + 1$ is again of that form ⟦as $(3n_1 + 1)(3n_2 + 1) = 3(n_1n_2 + n_1 + n_2) + 1$⟧. From this we deduce that any integer which is the product of prime factors of the form $3n+1$ only cannot be of the form $3n+2$. So by the Fundamental Theorem of Arithmetic we have a prime decomposition of $N = 3n + 2$ into prime factors, one of which is of type $3n$ or $3n + 2$. But the only prime of type $3n$ is 3, and this does not divide N. (Why?)
Now suppose there is a finite (exhaustive) list $\{p_1, \ldots, p_r\}$ of primes of the form $3n + 2$. Then take their product $M = p_1 \cdots p_r$ and consider $3M - 1$ (which obviously is > 2). By the above considerations, there must be at least one prime q of the form $3n + 2$ dividing $3M - 1 = 3(M - 1) + 2$. But any of the p_j $(j = 1, \ldots, r)$ is coprime to $3M - 1$, and hence to q. This contradicts the assumption that our list was exhaustive and proves the infinitude of primes of the form $3n + 2$.

(7) (a) For $n/2$ to be a square, all the exponents in a prime factorization of $n/2$ have to be even, and so

$$n/2 = 2^{2a_2} 3^{2a_3} 5^{2a_5} \cdots q^{2a_q}$$

for a_2, $a_3, \ldots, a_q \geq 0$, where q is the largest prime dividing n.
Similarly, for $n/3$ to be a cube, all exponents divisible by 3 and so

$$n/3 = 2^{3b_2} 3^{3b_3} 5^{3b_5} \cdots q^{3b_q}$$

for b_2, $b_3, \ldots, b_q \geq 0$.

Due to the Fundamental Theorem of Arithmetic, the unique prime decomposition implies

$$2a_2 + 1 = 3b_2\,, \qquad 2a_3 = 3b_3 + 1\,, \qquad 2a_5 = 3b_5\,, \ldots$$

For example, $a_2 = 1 = b_2$ and $a_3 = 2$ and $b_3 = 1$ and all the other a_j and b_j zero will do it, i.e. $n = 2^3 3^4$. Alternative solutions arise when we multiply this by any 6th power (> 0).

(b) Extending the above idea with a fifth power $n/5 = 2^{5b_2} 3^{5b_3} 5^{5b_5} \cdots q^{5b_q}$, we find $n = 2^{15} 3^{10} 5^6 \times$ a 30-th power.

(8) (a) It is the prime number 11.

(b) From question (2) we know that a composite number a has always a prime divisor p such that $p \leq \sqrt{a}$. Since here all integers are less than 100, the composite ones must have a prime factor not larger than $\sqrt{100}$, namely 10. The largest prime smaller than 10 is 7. This is why

the rest of the numbers have to be primes, since cannot contain any prime factor, different from them, larger than 7.

(9) (a) Note that the polynomial x^4+4 factors into $(x^2+2x+2)(x^2-2x+2)$ (i.e. as $(y-2x)(y+2x)$ for $y=x^2+2$, and so $y^2-(2x)^2=(x^2+2)^2-4x^2=x^4+4$). Now check that the first factor is >1 for any $x\geq 1$, and the second factor equals $(x-1)^2+1$, so is also >1, unless $x=1$.
This implies that x^4+4 is composite for $x>1$. (Clearly, it is a prime for $x=1$.)

(b) We show the contrapositive: if n is composite, then 2^n-1 is.
Write $n=a\cdot b$ for a, $b>1$, then check that $2^{ab}-1$ is divisible by (and clearly not equal to) 2^a-1, which is also >1. Indeed $\frac{2^{ab}-1}{2^a-1}=\frac{(2^a)^b-1}{2^a-1}=1+2^a+2^{2a}+\dots 2^{(b-1)a}$ by using the identity $\frac{x^n-1}{x-1}=1+x+\dots+x^{n-1}$.

(c) We first show that for an integer of the form $2^m\cdot p$ for a prime p and and $m\in\mathbb{N}$ the sum of its divisors is equal to $(p+1)(2^{m+1}-1)$.
We group the divisors d of $2^m\cdot p$ into two parts: the one for which p divides d, and the ones which don't. The latter ones are simply the powers of 2 of exponent 0, 1,..., n, while the former are the same ones multiplied by p.
Adding these up gives, for the first group, $1+2+2^2+\dots+2^m=2^{m+1}-1$, and $p(2^{m+1}-1)$ for the second, hence overall $(p+1)(2^{m+1}-1)$.
Now we consider the question. If the prime p is of the form 2^n-1, then we look at $N=\frac{p(p+1)}{2}=(2^n-1)2^{n-1}=p\cdot 2^{n-1}$. Applying the above computation gives for the sum of *all* divisors of N the number $(p+1)(2^n-1)=2^n(2^n-1)$, hence the sum of all divisors of N *other than itself* is indeed equal to
$2^n(2^n-1)-2^{n-1}(2^n-1)=2^{n-1}(2^n-1)=N$.

(10) A few preparations: it is easy to read off the gcd of two numbers if we have them in factored form: $\gcd(2^3\cdot 3^7\cdot 5^2\cdot 7, 2^5\cdot 3^2\cdot 7^{13})=2^3\cdot 3^2\cdot 7$, since we simply take the minimum of the respective exponents for all primes involved.

In general (with p_j primes and a_j, $b_j\geq 0$) one can check (why?) that:

$$\gcd\Big(\prod_{j=1}^r p_j^{a_j},\prod_{j=1}^r p_j^{b_j}\Big)=\prod_{j=1}^r p_j^{\min(a_j,b_j)}.$$

and

$$\operatorname{lcm}\Big(\prod_{j=1}^r p_j^{a_j},\prod_{j=1}^r p_j^{b_j}\Big)=\prod_{j=1}^r p_j^{\max(a_j,b_j)}.$$

In particular if we write $a=\prod_{j=1}^r p_j^{\alpha_j}$, and $b=\prod_{j=1}^r p_j^{\beta_j}$ then we have

$$\gcd(a,b)\operatorname{lcm}(a,b)=\prod_{j=1}^r p_j^{\min(a_j,b_j)}\times\prod_{j=1}^r p_j^{\max(a_j,b_j)}=\prod_{j=1}^r p_j^{\min(a_j,b_j)+\max(a_j,b_j)}=\prod_{j=1}^r p_j^{a_j+b_j}=ab$$

(11)

$$\gcd\Big(\prod_{j=1}^r p_j^{a_j},\prod_{j=1}^r p_j^{b_j},\prod_{j=1}^r p_j^{c_j}\Big)=\prod_{j=1}^r p_j^{\min(a_j,b_j,c_j)}.$$

$$\operatorname{lcm}\Big(\prod_{j=1}^{r} p_j^{a_j}, \prod_{j=1}^{r} p_j^{b_j}, \prod_{j=1}^{r} p_j^{c_j}\Big) = \prod_{j=1}^{r} p_j^{\max(a_j,b_j,c_j)}.$$

(a) Let $a = \prod_{j=1}^{r} p_j^{\alpha_j}$, $b = \prod_{j=1}^{r} p_j^{\beta_j}$, $c = \prod_{j=1}^{r} p_j^{\gamma_j}$. Then

$$\gcd(a,b,c) = \prod_{j=1}^{r} p_j^{\min(\alpha_j,\beta_j,\gamma_j)}$$

and

$$\gcd(\gcd(a,b),c) = \prod_{j=1}^{r} p_j^{\min(\min(\alpha_j,\beta_j),\gamma_j)}.$$

These two expressions coincide since $\min(\alpha,\beta,\gamma) = \min(\min(\alpha,\beta),\gamma)$. The equality with $\gcd(a,\gcd(b,c))$ is proved in the same way.

(b)

$$\operatorname{lcm}(a,b,c)\cdot\gcd(ab,bc,ca) = \prod_{j=1}^{r} p_j^{\max(\alpha_j,\beta_j,\gamma_j)} \cdot \prod_{j=1}^{r} p_j^{\min(\alpha_j+\beta_j,\beta_j+\gamma_j,\alpha_j+\gamma_j)}$$

Denote by $s_j := \alpha_j + \beta_j + \gamma_j$. Then $\alpha_j + \beta_j = s_j - \gamma_j, \alpha_j + \gamma_j = s_j - \beta_j$ and $\beta_j + \gamma_j = s_j - \alpha_j$. Without loss of generality assume that $\max(\alpha_j,\beta_j,\gamma_j) = \alpha_j$. Then $\min(s_j-\alpha_j, s_j-\beta_j, s_j-\gamma_j) = s_j - \alpha_j$ and therefore the sum of the min and max written above is always s_j. Finally we have

$$\operatorname{lcm}(a,b,c)\cdot\gcd(ab,bc,ca) = \prod_{j=1}^{r} p_j^{\max(\alpha_j,\beta_j,\gamma_j)+\min(\alpha_j+\beta_j,\alpha_j+\gamma_j,\beta_j+\gamma_j)} =$$

$$= \prod_{j=1}^{r} p_j^{\alpha_j+\beta_j+\gamma_j} = abc.$$