ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY II
SOLUTIONS OF PROBLEM SHEET 3
MICHAELMAS TERM 2014

(1) (a) Since $\gcd(3,11)=1$, we can write $1=3a+11b$ for some $a,b\in\mathbb{Z}$, and then $7a$ for any such a solves the problem $[\![1=3\cdot 4+11\cdot(-1),\quad x\equiv 7\cdot 4\equiv 6 \pmod{11}]\!]$.

(b) Again we have:

$$1=13\cdot 2-5\cdot 5;\quad x\equiv -15\equiv 11 \pmod{13}.$$

(2) (a) Apply the Euclidean Algorithm.

$$2011=3\cdot 663+22;$$

$$663=30\cdot 22+3;$$

$$22=7\cdot 3+1.$$

Therefore $\gcd(663,2011)=1$ and the linear congruence is solvable. The solution can be found as follows

$$1=22-7\cdot 3=22-7\cdot(663-30\cdot 22)$$

$$=211\cdot 22-7\cdot 663=211\cdot 2011-640\cdot 663.$$

Finally

$$x\equiv 151\cdot(-640)\equiv 1899 \pmod{2011}.$$

(b) Note that $3|1857$, $3|2013$ but $3\nmid 209$. Therefore $\gcd(1857,2013)\nmid 209$ and the congruence does not have solutions.

(3) (a) By a proposition from the lectures, since $\gcd(2,m)=1$ (by assumption), the "natural" complete set of residues modulo m, given by $\{0,1,\ldots,m-1\}$, when multiplied by 2, has still this property (of being complete).

(b) It is enough to prove that two integers in this set belong to the same class modulo m. We take 1 and $m-1$. Since $m>2$ we have that $(m-1)^2\equiv(-1)^2\equiv 1 \pmod{m}$. Hence the set is not a complete set of residues modulo m.

(4) Let $n\in\mathbb{N}$ bigger than 1 and write $n=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$ with $p_i\neq p_j$ for $i\neq j$, and $k_i>1$. The we observe that the positive divisors of n are given by $p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$ with $0\leq a_i\leq k_i$ for $i=1,2,\ldots,r$. Then we observe that $\tau(n)=(k_1+1)(k_2+1)\ldots(k_r+1)$ since this is the number of total divisors. For $\sigma(n)$ we claim that $\sigma(n)=\prod_{i=1}^{r}\frac{p_i^{k_i+1}-1}{p_i-1}$. Indeed if we consider the product

$$(1+p_1+p_1^2+\ldots+p_1^{k_1})(1+p_2+p_2^2+\ldots+p_2^{k_2})\ldots(1+p_r+p_r^2+\ldots+p_r^{k_r})$$

then every positive divisor of n appear once and only once as a term in the expansion of this product. In particular this product equals to $\sigma(n)$. Using the geometric series we can write every term in this product as

$$1 + p_i + p_i^2 + \ldots + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1},$$

and hence our claim follows. Using now these formulas it is easy to show that the functions are multiplicative. Indeed let us consider $m, n \in \mathbb{N}$ with $gcd(m, n) = 1$. If one of m or n is equal to one, it is clear since $\tau(1) = \sigma(1) = 1$. Hence we take $m, n > 1$. We moreover write $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ with $p_i \neq p_j$ for $i \neq j$, $k_i > 1$, and $m = q_1^{e_1} q_2^{e_2} \ldots q_s^{e_s}$ with $q_i \neq q_j$ for $i \neq j$, $e_i > 1$. Since $gcd(m, n) = 1$ we have that $p_i \neq q_j$ for all i, j. In particular we have that $nm = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} q_1^{e_1} q_2^{e_2} \ldots q_s^{e_s}$. Using the formulas above we have $\tau(n)\tau(m) = (k_1+1)(k_2+1)\ldots(k_r+1)(e_1+1)(e_2+1)\ldots(e_s+1)$. But also $\tau(nm) = (k_1+1)(k_2+1)\ldots(k_r+1)(e_1+1)(e_2+1)\ldots(e_s+1)$, and hence τ is multiplicative. Similarly we have $\sigma(n)\sigma(m) = \prod_{i=1}^{r} \frac{p_i^{k_i+1}-1}{p_i-1} \cdot \prod_{i=1}^{s} \frac{q_i^{e_i+1}-1}{q_i-1}$. But we also have $\sigma(nm) = \prod_{i=1}^{r} \frac{p_i^{k_i+1}-1}{p_i-1} \cdot \prod_{i=1}^{s} \frac{q_i^{e_i+1}-1}{q_i-1}$, and hence also σ is multiplicative.

They are not completely multiplicative. For example for p a prime we have $\tau(p^2) = 3$ but $\tau(p)\tau(p) = 2 \cdot 2 = 4 \neq 3$. Similarly we have $\sigma(p^2) = 1 + p + p^2$, and $\sigma(p)\sigma(p) = (1 + p)(1 + p) = 1 + 2p + p^2 \neq \sigma(p^2)$.

(5) We start by observeing that for $m, n \in \mathbb{N}$ with $gcd(m, n) = 1$ every positive divisor d of mn is of the form $d_1 d_2$ where $d_1 | m$ and $d_2 | n$, and d_1, d_2 positive, and $gcd(d_1, d_2) = 1$. We consider the function $F(n) = \sum_{0<d|n} f(d)$. Let m, n positive integers with $gcd(m, n) = 1$. We then have

$$F(mn) = \sum_{0<d|mn} f(d) = \sum_{0<d_1|m, 0<d_2|n, gcd(d_1,d_2)=1} f(d_1 d_2).$$

Using the multiplicativity of f we have that $f(d_1 d_2) = f(d_1) f(d_2)$, and hence

$$F(mn) = \left(\sum_{0<d_1|m} f(d_1) \right) \left(\sum_{0<d_2|n} f(d_2) \right) = F(m)F(n).$$

Hence F is multiplicative.

We can conclude again that τ and σ are multiplicative by writing $\tau(n) = \sum_{0<d|n} 1$ and $\sigma(n) = \sum_{0<d|n} d$. Since the functions $f_1(n) = 1$ and $f_2(n) = n$ are obviously multiplicative so is also τ and σ.

(6) (a) Using the formula $\varphi(n) = n \prod_{p|n}(1 - p^{-1})$, we get
$\varphi(275) = 275 \cdot \frac{4}{5} \cdot \frac{10}{11} = 200$.

(b) In this case, we can also use the simple formula for prime powers
$\varphi(2^7) = 2^7 - 2^6 = 2^6 (= 64)$.

(c) Above formula again gives
$\varphi(404) = 404 \cdot \frac{1}{2} \cdot \frac{100}{101} = 200$,
i.e. the same value as for (i), despite their rather different prime decompositions.

(7) (a) For $\varphi(n)$ odd, say $n = p_1^{k_1} \cdots p_r^{k_r}$ we get

$$\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1)\,.$$

If *any* p_j $(1 \le j \le r)$ is odd, then $p_j - 1$ is even, and so $\varphi(n)$ is. Therefore n must be of the form $n = 2^k$, and we have

$$\varphi(2^k) = \begin{cases} 2^{k-1} & k \ge 1 \\ 1 & k = 0 \end{cases}$$

which is odd only if $k = 1$ (i.e. for $n = 2$) and for $k = 0$ (i.e. for $n = 1$).

(b) For $n = p_1^{k_1} \cdots p_r^{k_r}$ (where the p_j $(j = 1, \ldots, r)$ denote different primes) we can write

$$\varphi(n) = p_1^{k_1} \cdots p_r^{k_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

and so the condition $\varphi(n) = n/2$ boils down to satisfying the equation

$$\frac{1}{2} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)\,.$$

Clearly, 2 has to occur as one of the prime factors p_j ⟦multiply both sides by $2p_1 \cdots p_r$ to get an equation among integers and then apply a result [due to Euklid] from an early lecture⟧. Hence, putting $p_1 = 2$ we find

$$\frac{1}{2} = \frac{1}{2}\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)\,.$$

But this is only possible if no other prime on the RHS occurs, since each factor $(1 - 1/p_j)$ $(j = 2, \ldots, r)$ would make the product on the right smaller than the number on the left.

Conclusion: n has to be divisible by 2, and no other prime divides n. Hence the set of all n such that $\varphi(n) = n/2$ is given by $\{2^k \mid k \ge 1\}$.

(c) Similarly, the condition $\varphi(n) = n/3$ boils down to

$$\frac{1}{3} = (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})\,.$$

Using the same argument as before, 3 has to occur as one of the prime factors p_j. Hence we can put $p_1 = 3$ (note that we do not order the p_j here) and write

$$\frac{1}{3} = \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) = \frac{2}{3}\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)\,.$$

Multiplying both sides by $3/2$, we obtain the equation

$$\frac{1}{2} = \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

which is essentially the one dealt with in the previous case.

Conclusion: both 3 and 2 must occur as prime factors, and this is indeed sufficient (check!).

Hence the set of n with $\varphi(n) = n/3$ is given by $\{2^k \cdot 3^\ell \mid k, \ell \ge 1\}$.

(8) (a) We know from Fermat's Little Theorem that, since $\gcd(9, 67) = 1$, we have

$$a^{66} \equiv 1 \pmod{67}.$$

By taking higher powers we get

$$(a^{66})^k \equiv 1 \pmod{67} \qquad \text{any } k \geq 0.$$

Now $728 = 11 \cdot 66 + 2$, so we find

$$9^{728} = 9^{11 \cdot 66 + 2} \equiv (9^{66})^{11} \cdot 9^2 \equiv 9^2 \equiv 14 \pmod{67}.$$

So $a = 14$.

(b) Sine 6 and 10 are not coprime then Fermat Little Theorem (together with Euler Theorem) is not applicable. On the other hand just note that

$$6^2 \equiv 6 \pmod{10}; \quad 6^3 \equiv 6 \pmod{10}, \ldots...$$

$$6^n \equiv 6^{n-1} \cdot 6 \equiv 6 \pmod{10}$$

for every positive integer n. Therefore the last digit of 6^{166} is 6.

(c) Since $\varphi(10) = 4$ then by Euler Theorem we have $7^4 \equiv 1 \pmod{10}$. Then if we divide 7^{77} by 4 with the remainder (i.e. $7^{77} = 4k + r$) then we get

$$7^{7^{77}} \equiv 7^{4k+r} \equiv (7^4)^k \cdot 7^r \equiv 7^r \pmod{10}.$$

In order to find r we need to calculate $7^{77} \pmod 4$. Euler Theorem in this case gives us $7^2 \equiv 1 \pmod 4$ and therefore

$$7^{77} \equiv 7 \equiv 3 \pmod 4.$$

Finally

$$7^{7^{77}} \equiv 7^3 \equiv 3 \pmod{10}.$$

(9) (a) By Fermat's Little Theorem, we know that, for any x with $\gcd(x, 29) = 1$, we have $x^{28} \equiv 1 \pmod{29}$, as 29 is prime. Hence also $(x^{28})^3 \equiv 1 \pmod{29}$ and so $x^{86} \equiv x^{3 \cdot 28} \cdot x^2 \equiv x^2 \pmod{29}$.
In order to solve $x^2 \equiv 6 \pmod{29}$, it suffices to check that $2 \cdot 29 + 6 = 8^2$, so the congruence transforms to

$$x^2 \equiv 8^2 \pmod{29}.$$

By subtracting 8^2 from both sides we get $29|(x - 8)(x + 8)$ which in view of primality of 29 implies $29|(x - 8)$ or $29|(x + 8)$. Finally we get

$$x \equiv \pm 8 \equiv 8, 21 \pmod{29}.$$

(b) For any integer x we have $x^{13} \equiv x \pmod{13}$.
Hence $x^{39} = (x^{13})^3 \equiv x^3 \pmod{13}$. Therefore we get

$$x^3 - 2^3 = (x - 2) \cdot (x^2 + 2x + 4) \equiv 0 \pmod{13}.$$

In other words $13|(x - 2)(x^2 + 2x + 4)$. From here we get either $x \equiv 2 \pmod{13}$ or $x^2 + 2x + 4 \equiv 0 \pmod{13}$. For the last congruence we just write it as

$$(x + 1)^2 \equiv 10 \equiv 36 \pmod{13}.$$

By the same arguments as in part (a) the solution to the last congruence is $x+1 \equiv \pm 6 \pmod{13}$. So the final answer is

$$x \equiv 2, 5, 6 \pmod{13}.$$

(10) Fermat says: for any prime p and any integer a with $\gcd(a,p) = 1$ ⟦don't forget!⟧we have

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

(a) Let $a = 7$ and $m = 1734251$; we find $\gcd(a,m) = 1$.
If m were prime, then the right hand side would have to be 1 (which it isn't). Hence we can indeed conclude that m is composite.

(b) Yes: suppose $p = 64027$ were a prime, then $\varphi(p) = p - 1 = 64026$, and by Fermat any a with $0 < a < p$ (which hence clearly satisfies $\gcd(a,p) = 1$) would have to satisfy $a^{64026} \equiv 1 \pmod{64027}$. Obviously, 29670 is not congruent $1 \pmod{64027}$, and hence 64027 cannot be prime.

(c) Clearly $\gcd(2, 52633) = 1$, so by Fermat we get that *if* 52633 is prime, then indeed $2^{52632} \equiv 1 \pmod{52633}$. But it does not tell us anything about the converse, so we cannot conclude from Fermat alone that 52633 is prime. Indeed, it isn't (one factor is 7, the others 73, 103).

(11) We have to assume $n > 4$, since obviously $(4-1)! = 6$ is *not* congruent $0 \pmod 4$.
Let n be composite, then $n = ab$ for some a, $b > 1$. Clearly both a and b are also smaller than n.
If $a \neq b$, then it is evident that they both occur as factors of $(n-1)!$ in the obvious way, so n divides the latter.
If $a = b > 2$, we have $2a < ab$ and both a and $2b (= 2a)$ occur as *different* factors of $(n-1)!$, and in particular the latter is divisible by $n = ab$.

(12) By Wilson's Theorem for the prime p, we get

$$\underbrace{1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)}_{\text{first half}} \cdot \underbrace{\left(\frac{p+1}{2}\right) \cdot \left(\frac{p+3}{2}\right) \cdots (p-1)}_{\text{second half}} \equiv -1 \pmod{p},$$

and each factor of the second half complements precisely one factor of the first half to p, so we can pair them off to

$$\underbrace{1(p-1)} \cdot \underbrace{2(p-2)} \cdots \underbrace{\left(\frac{p-1}{2}\right)\left(p - \frac{p-1}{2}\right)}.$$

But since $p - j \equiv -j \pmod{p}$, we can write this expression as

$$1^2 \cdot 2^2 \cdots \left(\frac{p-1}{2}\right)^2 \cdot (-1)^{(p-1)/2}$$

(each product $j(p-j)$ is $\equiv -j^2 \pmod{p}$, hence contributes a minus sign).

Now since $p \equiv 3 \pmod 4$, $(p-1)/2$ is odd and so $(-1)^{(p-1)/2} = -1$, and we find

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

Finally, for an odd prime p the only two numbers modulo p whose square is $+1$ are given by 1 and -1, hence $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}$.

(13) (a) We write $1 = a \cdot 5 + b \cdot 11$ with $a = -2$ and $b = 1$. Hence

$$\begin{aligned} 3 &= 3 \cdot (-2) \cdot 5 + 3 \cdot 11\,, \\ 7 &= 7 \cdot (-2) \cdot 5 + 7 \cdot 11\,. \end{aligned}$$

Define $x = 7 \cdot (-2) \cdot 5 + 3 \cdot 11 = -37 \equiv 18 \pmod{55}$. This solves the congruence by the algorithm in the proof of the Chinese Remainder Theorem.
Check indeed that $18 \equiv 3 \pmod 5$ and $18 \equiv 7 \pmod{11}$.
In fact, any number $18 + 55k$, with $k \in \mathbb{Z}$, solves the simultaneous congruence.

(b) We write $1 = a \cdot 37 + b \cdot 87$ with $a = 40$ and $b = -17$. (E.g., use Euclidean algorithm.). Hence

$$\begin{aligned} 3 &= 3 \cdot 40 \cdot 37 + 3 \cdot (-17) \cdot 87\,, \\ 1 &= 40 \cdot 37 + (-17) \cdot 87\,. \end{aligned}$$

Define $x = 40 \cdot 37 + 3 \cdot (-17) \cdot 87 = 1480 - 3 \cdot 1479 = 1 - 2 \cdot 1479 = -2957$. This does it. A positive solution is e.g. 262.

(c) We define $n = 7 \cdot 12 \cdot 13 = 1092$, and $N_1 = 12 \cdot 13 = 156$, $N_2 = 7 \cdot 13 = 91$ and $N_3 = 7 \cdot 12 = 84$. We solve the congruences $156x_1 \equiv 1 \pmod 7$, $91x_2 \equiv 1 \pmod{12}$, and $84x_3 \equiv 1 \pmod{13}$. This can be done using the Euclidean algorithm as we have seen in the lectures, and in exercises (1) and (2). Solutions are $x_1 = -3$, $x_2 = -5$, and $x_3 = -2$. Hence a solution to our system is given by

$$x = -3 \cdot 156 \cdot 5 + (-5) \cdot 91 \cdot 3 + (-2) \cdot 84 \cdot 8 = -5049 \equiv -681 \equiv 411 \pmod{1092}.$$

(14) We consider the system $x \equiv 3 \pmod{17}$, $x \equiv 10 \pmod{16}$ and $x \equiv 0 \pmod{15}$. We can solve it as in the previous question.