ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY II
SOLUTIONS FOR PROBLEM SHEET 4
MICHAELMAS TERM 2014

(1) (a) For the last 2 digits result when we should take congruences modulo 100.
Since $\varphi(100) = 100 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$, we have

$$3^{40} \equiv 1 \pmod{100}$$

by Euler–Fermat, and hence the same holds for the tenth powers of the LHS.

(b) Successive squaring gives:

$$5^2 \equiv 2 \pmod{23}, \qquad 5^4 \equiv 4 \pmod{23}, \qquad 5^8 \equiv 16 \pmod{23},$$

and hence

$$5^{13} = 5^{8+4+1} = 5^8 \cdot 5^4 \cdot 5 \equiv \underbrace{16 \cdot 4}_{\equiv -5} \cdot 5 \equiv -25 \equiv 21 \pmod{23}.$$

(c) To make calculations slightly shorter we notice that $2011 \equiv -2 \pmod{2013}$ Then repeat the same procedure as before.

k	0	1	2	3	4	5	6	7	8	9	10
$(-2)^{2^k}$	-2	4	16	256	1120	301	16	256	1120	301	16

(Note that after $k = 6$ the sequence $(-2)^{2^k} \pmod{2013}$ becomes periodic.) Hence we read off

$$(-2)^{2012} \equiv 16 \cdot 256 \cdot 1120 \cdot 16 \cdot 256 \cdot 1120 \cdot 301 \cdot 16 \equiv 301 \pmod{2013}.$$

(2) (a) We know, as a consequence of Fermat, that $2^{k \cdot 16} \equiv 1 \pmod{17}$. The algorithm for computing kth roots modulo m in the lectures suggested (here $r = 2$, $k = 11$, $m = 17$) first to compute $\varphi(m)$ (here $= 16$), then to find an a with $1 \leq a \leq \varphi m$, such that $ak \equiv 1 \pmod{\varphi(m)}$. Here we have $a = 3$ suffice), and then to compute $r^a \pmod{m}$ (here $2^3 = 8$). Indeed 8^{11} can be written as 8^{8+2+1}, and we get, by successive squaring, $8^2 \equiv 13$, $8^4 \equiv 13^2 = 169 \equiv -1$ and $8^8 \equiv 1 \pmod{17}$, so $8^{11} \equiv 8 \cdot 13 = 104 \equiv 2 \pmod{17}$.

(b) As above we get $\varphi(23) = 22$ and then by Euclidean algorithm we find$1 = 7 \cdot 22 - 9 \cdot 17$. Hence we have $a \equiv -9 \equiv 13 \pmod{22}$. Hence we have that a solution given by (note that the computations below have been done in 1(b)
$x \equiv 5^{13} \equiv 21 \pmod{23}$.

(c) $\varphi(29) = 28$, $\quad 1 = 1 \cdot 28 - 3 \cdot 9 = 25 \cdot 9 - 8 \cdot 28$,

$$x \equiv 12^{25} \pmod{29}.$$

We can calculate it by the method of successive squaring:

k	0	1	2	3	4
12^{2^k}	12	28	1	1	1

So $x \equiv 12^{25} \equiv 12 \pmod{29}$.

x can also be calculated by using value $a = -3$ instead of $a = 25$: $x \equiv 12^{-3} \equiv 12 \pmod{29}$. To calculate the negative power we need to solve the linear congruence $12^3 x \equiv 1 \pmod{29}$.

(3) There are four solutions to this congruence: $x \equiv 3, 9, 15, 21 \pmod{24}$. To get this one can either use the brute force or use the following arguments:

$$x^2 - 9 = (x-3)(x+3) \equiv 0 \pmod{24}.$$

Therefore $24|(x-3)(x+3)$. Now consider each prime factor from the factorization of 24 separately. From $3|(x-3)(x+3)$ we have that either $x \equiv 3 \pmod 3$ or $x \equiv -3 \pmod 3$. In both cases we get $x \equiv 0 \pmod 3$. Finally note that each odd number x satisfy $8|(x-3)(x+3)$. Hence the solutions x should satisfy $x \equiv 0 \pmod 3$ and $x \equiv 1 \pmod 2$ which, modulo 24, gives us the results above.

Remark. Here we see that the number of solutions modulo 24 is bigger than the degree of the congruence. It shows that for the composite modules the theorem of Lagrange from the lectures is not true.

(4) An inverse of 3 in $\mathbb{Z}/22\mathbb{Z}$ is given by -7, as $3(-7) = -21 \equiv 1 \pmod{22}$. Now $x = -7 \equiv 15 \pmod{22}$ satisfies

$$8^x \equiv (2^3)^x = 2^{3x} \equiv 2^{45} \equiv 2^{22} \cdot 2 \equiv 2 \pmod{23},$$

the last congruence due to Fermat.

(5) (a) We have

$$\operatorname{ord}_{13}(5) = 4 \qquad \text{use, e.g. } 5^2 \equiv -1 \pmod{13}),$$

and

$$\operatorname{ord}_{13}(7) = 12.$$

It suffices to check that $7^4 = (7^2)^2 \equiv (-3)^2 \not\equiv 1 \pmod{13}$ and $7^6 = 7^4 \cdot 7^2 \equiv 9 \cdot (-3) \not\equiv 1 \pmod{13}$, since the order of 7 modulo 13 must divide $\varphi(13) = 12$.

Furthermore, we have

$$\operatorname{ord}_{13}(9) = 3 \qquad \text{use, e.g. } 9 \cdot 9^2 \equiv 9 \cdot 3 \equiv 1 \pmod{13}).$$

(b) The order of 11 modulo 641 must divide $640 = 2^7 \cdot 5$, so we look at all the binary powers 2^k of both 11 and of 11^5 for $k = 0, \ldots, 7$, using our squaring method.
We get for

$$11^{2^2} \equiv 539 \equiv -102 \pmod{641},$$

and hence

$$11^5 \equiv (-102) \cdot 11 = -1122 \equiv 160 \pmod{641}$$

together with its inverse

$$11^{-5} \equiv -4 \pmod{641}.$$

For the further binary powers of 11, we find

$$11^{2^3} = (11^4)^2 \equiv (-102)^2 \equiv 148 \pmod{641},$$
$$11^{2^4} \equiv 148^2 \equiv 110 \pmod{641},$$
$$11^{2^5} \equiv 110^2 \equiv 562 \pmod{641},$$
$$11^{2^6} \equiv 562^2 \equiv 472 \pmod{641},$$
$$11^{2^7} \equiv 472^2 \equiv 357 \pmod{641}.$$

None of the above is 1 (mod 641), hence 5 must divide $\mathrm{ord}_{641}(11)$. We now compute the powers of 11^5. Since the order of 11 is the same as the order of 11^{-1}, we could just as well take successive squares of $11^{-5} \equiv -4$, which is simpler:

$$(11^{-5})^2 \equiv 16, \quad (11^{-5})^4 \equiv 256, \quad (11^{-5})^8 = 65536 \equiv 154 \pmod{641};$$

now squaring the latter gives $(11^{-5})^{16} \equiv 154^2 \equiv -1 \pmod{641}$, and so, without further squaring we can already deduce that the order of 11^{-1}, and hence also of 11, is $5 \cdot 32$, hence 160.

(6) We find $\mathrm{ord}_{21}(2) = 6$ (look at the orders of the individual prime powers dividing the modulus 21, and take the lcm of the results).

Furthermore, for $\mathrm{ord}_{25}(2)$ we have to check only the powers of two with exponent dividing $\varphi(25) = 20$, i.e., exponents $1, 2, 4, 5, 10$. The corresponding powers (i.e., 2, 4, 16, 32, 1024), are clearly $\not\equiv 1 \pmod{25}$ hence we can deduce $\mathrm{ord}_{25}(2) = 20$.

For $\mathrm{ord}_{32}(3)$, we only need to check the powers 1, 2, 4, 8 (all the divisors of $\varphi(32) = 16$ different from 16 itself), giving the numbers 3, 9, $81 \equiv -15$, $(-15)^2 = 225 \equiv 1 \pmod{32}$. Hence the order is $\mathrm{ord}_{32}(3) = 8$.

Finally, the order of 3 modulo 7 is 6, and its order modulo 2 is equal to 1, hence $\mathrm{ord}_{14}(3) = \mathrm{lcm}(6, 1) = 6$. (Indeed, $3^6 = 27^2 \equiv (-1)^2 = 1 \pmod{14}$, but neither 3^2 nor 3^3 satisfies that congruence.)

(7) (a) We'll try different numbers between 2 and 16 one by one until we find a number a such that $ord_{17}(a) = 16$. Since $ord_{17}(a)|16$ so the candidates for the order are the powers of 2 only.
Let's firstly try $a = 2$:

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^4 \equiv 16 \equiv -1,\ 2^8 \equiv 1 \pmod{17}.$$

Therefore $\mathrm{ord}_{17}(2) = 8$. Next try $a = 3$:

$$3^1 \equiv 3,\ 3^2 \equiv 9\ 3^4 \equiv 13,\ 3^8 \equiv 16,\ 3^{16} \equiv 1 \pmod{17}.$$

Therefore 3 is the primitive root modulo 17.

(b) We proceed as before. In this case $\varphi(23) = 22 = 2 \cdot 11$. So to be sure that given a is a primitive root we need to check that $a^2 \not\equiv 1 \pmod{23}$ and $a^{11} \not\equiv 1 \pmod{23}$.
For $a = 2$ we have $2^{11} \equiv 1 \pmod{23}$. So 2 is not a primitive root.
For $a = 3$ we also have $3^{11} \equiv 1 \pmod{23}$. We do not need to check $a = 4$ since $4 = 2^2$ and 2 is not a primitive root. The next candidate is 5:

$$5^2 \equiv 2 \pmod{23}, \quad 5^{11} \equiv 22 \pmod{23}.$$

Therefore 5 answers the question.

(8) (a) Suppose first that $k \equiv 0 \pmod{ord_n(a)}$. Then we can write $k = mord_n(a)$ for some integer m. Then we have

$$a^k \equiv a^{mord_n(a)} \equiv (a^{ord_n(a)})^m \equiv 1^m \equiv 1 \pmod{n}.$$

For the other direction, assuming that $a^k \equiv 1 \pmod{n}$ using the division with remainder we write $k = qord_n(a) + r$ with $q \in \mathbb{Z}$ and $0 \leq r < ord_n(a)$. But then we have that $1 \equiv a^k \equiv a^{qord_n(a)}a^r \equiv (a^{ord_n(a)})^q a^r \equiv a^r \pmod{n}$. Hence $a^r \equiv 1 \pmod{n}$, and $0 \leq r < ord_n(a)$. Hence $r = 0$, and so $k \equiv 0 \pmod{n}$.

(b) We define $d := gcd(b, ord_n(a))$. Then we may write $b = b_1 d$ and $ord_n(a) = kd.$ with $gcd(b_1, k) = 1$. Then we have

$$(a^b)^k \equiv (a^{b_1 d})^{ord_n(a)/d} \equiv (a^{ord_n(a)})^{b_1} \equiv 1 \pmod{n}.$$

From this and (a) above we conclude that $ord_n(a^b)|k$. On the other hand we have that

$$a^{bord_n(a^b)} \equiv (a^b)^{ord_n(a^b)} \equiv 1 \pmod{n},$$

and hence again by (a) we have $ord_n(a)|bord_n(a^b)$. That is $kd|b_1 dord_n(a^b)$ or equivalently $k|b_1 ord_n(a^b)$. But $gcd(k, b_1) = 1$ and hence $k|ord_n(a^b)$. Hence we can conclude that $ord_n(a^b) = k = ord_n(a)/d$.

(9) Since $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$ we have that $2^{2^{n+1}} \equiv 1 \pmod{F_n}$. Hence the order of 2 modulo F_n is not larger than 2^{n+1}. But since we assume that F_n is a prime, we have that

$$\varphi(F_n) = F_n - 1 = 2^{2^n},$$

and it is easy to see that $2^{2^n} > 2^{n+1}$ for $n > 1$. Hence the order of 2 modulo F_n is smaller than $\varphi(F_n)$. Hence 2 is not a primitive root modulo F_n.

(10) (a) We write $d = gcd(\varphi(m), \varphi(n))$. By Question 7(a) in Problem Sheet 3 we know that both $< varphi(m)$ and $\varphi(n)$ are even since $m, n > 2$, and hence $d \geq 2$. Moreover by Question 10 in Problem Sheet 2 we have that $bd = \varphi(m)\varphi(n)$. In particular we have that $b = \frac{\varphi(m)\varphi(n)}{d} \leq \frac{\varphi(m)\varphi(n)}{2}$.

(b) We have by using Eulers Theorem that

$$a^b \equiv (a^{\varphi(m)})^{\varphi(n)/d} \equiv 1^{\varphi(n)/d} \equiv 1 \pmod{m},$$

and

$$a^b \equiv (a^{\varphi(n)})^{\varphi(m)/d} \equiv 1^{\varphi(m)/d} \equiv 1 \pmod{n}$$

(c) We have shown that $a^b \equiv 1 \pmod{m}$ and $a^b \equiv 1 \pmod{n}$, and since $gcd(n, m) = 1$ we have also that $a^b \equiv 1 \pmod{nm}$. But by (a) we have that $b \leq \frac{\varphi(m)\varphi(n)}{2} = \frac{\varphi(nm)}{2} < \varphi(nm)$. And this hold for all $a \in \mathbb{Z}$ with $gcd(a, mn) = 1$. In particular there exist no primitive root modulo nm with $n, m > 2$ and $gcd(n, m) = 1$.

(11) (a) We get the following table

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$I(a)$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

(b) We solve $13x \equiv 6 \pmod{17}$ by working with index calculus: the equation is transformed to

$$I(13) + I(x) \equiv I(6) \pmod{\varphi(17)},$$

i.e.,

$$4 + I(x) \equiv 15 \pmod{16},$$

hence $I(x) = 11$, for which we read off from the above table $x = 7$. [Check gives $13 \cdot 7 = 91 \equiv 6 \pmod{17}$, indeed.]

(c) Similarly, we solve $5x^7 \equiv 7 \pmod{17}$ by applying I to both sides and using the rules of index calculus: we get

$$I(5) + 7I(x) \equiv I(7) \pmod{16},$$

hence (using $I(5) = 5$ and $I(7) = 11$)

$$7I(x) \equiv 6 \pmod{16}.$$

Noting that 7 is its own inverse modulo 16 (as $7 \cdot 7 \equiv 1 \pmod{16}$), we need to find x such that $I(x) = 42 \equiv 10 \pmod{16}$, whence $x = 8$. [Check gives $5 \cdot 8^7 = 5 \cdot 2^{21} \equiv 5 \cdot 2^5 = 160 \pmod{17}$, and we only need to check that $153 (= 160 - 7)$ is indeed divisible by 17.]