Exercises 2 for KAP: solutions
Laura Geatti - Lea Terracini

Problem 1. *For each of the following groups*

$$\mathbb{Z}/12\mathbb{Z}, \quad (\mathbb{Z}/100\mathbb{Z})^*, \quad \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}, \quad \mathbb{Z}/11\mathbb{Z} \times (\mathbb{Z}/17\mathbb{Z})^*, \quad (\mathbb{Z}/7^3\mathbb{Z})^*$$

(a) determine the order;

(b) list the possible orders of its elements;

(c) choose an element in the group ($\neq 1$) and verify that (2.) of Corollary 4.9 in the Algebra notes holds true.

Solution. • Let $G = \mathbb{Z}/12\mathbb{Z}$.
G is an additive group of order 12. The order of an element $x \in G$ is a divisor of 12. Since the group is cyclic, for every divisor d of 12 there are precisely $\varphi(d)$ elements of order d (here φ denotes the Euler function). Let $\bar{x} = \bar{5} \in \mathbb{Z}/12\mathbb{Z}$. The multiples of 5 modulo 12 are

$$5, \quad 2 \cdot 5 = 10, \quad 3 \cdot 5 \equiv 3, \quad 4 \cdot 5 \equiv 8, \quad 5 \cdot 5 \equiv 1, \quad 6 \cdot 5 \equiv 6,$$

$$7 \cdot 5 \equiv 11, \quad 8 \cdot 5 \equiv 4, \quad 9 \cdot 5 \equiv 9, \quad 10 \cdot 5 \equiv 2, \quad 11 \cdot 5 \equiv 7, \quad 12 \cdot 5 \equiv 0.$$

Hence the order of $\bar{5}$ in the additive group $\mathbb{Z}/12\mathbb{Z}$ is 12.

• Let $G = (\mathbb{Z}/100\mathbb{Z})^*$.
G is a multiplicative group of order $\varphi(100) = \varphi(2^2)\varphi(5^2) = 40$. By the Chinese Remainder Theorem

$$(\mathbb{Z}/100\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/25\mathbb{Z})^*,$$

where $\#(\mathbb{Z}/4\mathbb{Z})^* = 2$ and $\#(\mathbb{Z}/25\mathbb{Z})^* = 20$. Hence the order of an element $x \in G$ is a divisor of $lcm(2, 20) = 20$. Take for example $\bar{3} \in (\mathbb{Z}/100\mathbb{Z})^*$. Then its powers are

$$\bar{3}, \quad \bar{3}^2 = \bar{9}, \quad , \bar{3}^3 = \overline{27}, \quad \bar{3}^4 = \overline{81}, \quad \bar{3}^5 = \overline{43}, \quad \bar{3}^6 = \overline{29}, \quad \bar{3}^7 = \overline{87}$$

$$\bar{3}^8 = \overline{61}, \quad \bar{3}^9 = \overline{83}, \quad \bar{3}^{10} = \overline{49}.$$

Since the divisors of 20 are $\{1, 2, 4, 5, 10, 20\}$ and $\bar{3}^{10} \neq \bar{1}$, then order of $\bar{3}$ is necessarily 20.

• Let $G = \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$.
The group G is an additive group of order 187. Since $\gcd(11, 17) = 1$, G is isomorphic to the cyclic group $\mathbb{Z}/187\mathbb{Z}$. The order of an element $x \in G$ is a divisor of $lcm(11, 17) = 11 \cdot 17 = 187$, that is an integer in $\{1, 11, 17, 187\}$.
For example, the order of $(\bar{0}, \bar{0})$ is 1. The order of $(\bar{1}, \bar{1}) \in \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$ is exactly 187, the order of $(\overline{11}, \bar{1})$ is 17, the order of $(\bar{1}, \overline{17})$ is 11.

• Let $G = \mathbb{Z}/11\mathbb{Z} \times (\mathbb{Z}/17\mathbb{Z})^*$.
The group G is the direct product of an additive cyclic group of order 11 and a multiplicative cyclic group of order $\varphi(17) = 16$. The neutral element of G is $(\bar{0}, \bar{1})$. The order of an element $x \in G$ is a divisor of $lcm(11, 16) = 11 \cdot 16 = 176 = 2^4 \cdot 11$, that is an integer in the set $\{1, 2, 4, 8, 16, 11, 22, 44, 88, 176\}$.
For example, let's take the element $(\bar{0}, \bar{2}) \in G$. Since

$$(2 \cdot \bar{0}, \bar{2}^2) = (\bar{0}, \bar{4}), \quad (3 \cdot \bar{0}, \bar{2}^3) = (\bar{0}, \bar{8}), \quad (4 \cdot \bar{0}, \bar{2}^4) = (\bar{0}, \overline{16}) = (\bar{0}, \overline{-1}),$$

then $(8 \cdot \bar{0}, \bar{2}^8) = (\bar{0}, \bar{2}^4 \cdot \bar{2}^4) = (\bar{0}, \bar{1})$ and the order of $(\bar{0}, \bar{2})$ is 8.

• Let $G = (\mathbb{Z}/7^3\mathbb{Z})^* = (\mathbb{Z}/343\mathbb{Z})^*$.
The group G is a multiplicative group of order $7^3 - 7^2 = 294 = 2 \cdot 3 \cdot 7^2$. Since $(\mathbb{Z}/7^3\mathbb{Z})^*$ is cyclic, the possible orders of its elements are precisely the divisors of 294, namely

$$\{1, 2, 3, 6, 7, 14, 21, 42, 49, 98, 147, 294\}.$$

For example, let's take the element $\overline{13} \in G$. Since

$$13^{98} \equiv 1 \pmod{343},$$

the order of $\overline{13}$ is a divisor of $98 = 2 \cdot 7^2$. Hence it is an integer in the set $\{2, 7, 14, 49, 98\}$. One checks that

$$13 \not\equiv 1, \quad 13^2 \equiv 169, \quad 13^7 \equiv 97, \quad 13^{14} \equiv 148, \quad 13^{49} \equiv -1 \pmod{343}.$$

Hence the order of $\overline{13}$ is indeed 98.

Problem 2. *Let $n \in \mathbb{N}$. Show that*

(a) Verify that $\varphi(n)$ is even, for every integer $n > 2$;

(b) if a prime p divides n, then $\varphi(p)$ divides $\varphi(n)$;

(c) if p^2 does not divide n, then $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$;

(d) if p divides $\frac{n}{p}$, then $\varphi(\frac{n}{p}) = \frac{n}{p}\prod_{d|n}(1 - \frac{1}{d})$, where d varies in the set of distinct prime divisors of n.

Solution. (a) If $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, then

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \dots \varphi(p_k^{a_k}), \qquad \text{where } \varphi(p_j^{a_j}) = p_j^{a_j - 1}(p_j - 1).$$

If $n > 2$, then n is divisible either by 2^m, with $m > 1$, or by an odd prime $p > 2$. In both cases $\varphi(n)$ is even.

(b) By the above expression of $\varphi(n)$ it is clear that if a prime p divides n, then $\varphi(p)$ divides $\varphi(n)$.

(c) If p^2 does not divide n, then p appears with exponent 1 in the prime decomposition of n and $\gcd(p, \frac{n}{p}) = 1$. Now from the Chinese Remainder Theorem it follows that $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$.

(d) One has

$$\varphi(n) = n \prod_{d|n} \left(1 - \frac{1}{d}\right),$$

where d runs through the prime divisors of n. If p divides $\frac{n}{p}$, then n and $\frac{n}{p}$ have the same prime divisors. It follows that

$$\varphi\left(\frac{n}{p}\right) = \frac{n}{p} \prod_{d|\frac{n}{p}} \left(1 - \frac{1}{d}\right) = \frac{n}{p} \prod_{d|n} \left(1 - \frac{1}{d}\right).$$

Problem 3. *Let* $\bar{x} = \overline{222487}$ *and* $\bar{y} = \overline{46375}$.
Determine the orders of $\bar{x}$ *and* $\bar{y}$ *in the groups*

$$\mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/35\mathbb{Z}, \quad \mathbb{Z}/7\mathbb{Z}, \quad \mathbb{Z}/11\mathbb{Z}.$$

Solution. • In $\mathbb{Z}/3\mathbb{Z}$, one has $\bar{x} = \bar{y} = \bar{1}$. The order of $\bar{1}$ in the additive group $\mathbb{Z}/3\mathbb{Z}$ is 3.

• In $\mathbb{Z}/35\mathbb{Z}$, one has $\bar{x} = \overline{27}$ and $\bar{y} = \bar{0}$. Since $\gcd(27, 35) = 1$, the order of $\bar{x}$ is 35. The order of $\bar{y}$ is 1.

• In $\mathbb{Z}/7\mathbb{Z}$, one has $\bar{x} = \overline{6} = \overline{-1}$ and $\bar{y} = \bar{0}$. Since $\gcd(7, -1) = 1$, the order of $\bar{x}$ is 7. The order of $\bar{y}$ is 1.

• In $\mathbb{Z}/11\mathbb{Z}$, one has $\bar{x} = \overline{1}$ and $\bar{y} = \overline{10} = \overline{-1}$. The order of $\bar{x}$ is 11. The order of $\bar{y}$ is 11.

Problem 4. *Let* $n = 1517$.

(a) Prove that for all $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$, *the order of* $\bar{x}$ *is equal to* $\frac{n}{\gcd(x,n)}$.

(b) Determine the order of $\bar{x} = \overline{185}$ *in* $\mathbb{Z}/n\mathbb{Z}$.

Solution. (a) We apply the following fact:
Let G be a cyclic group of order n, let g be a generator of G (i.e. an element of order n), and let a be an integer. Then

$$ord(g^a) = \frac{n}{\gcd(a, n)}.$$

To see this, let k be the order of g^a, that is the smallest integer such that $(g^a)^k = g^{ak} = 1$. Since g is a generator, then n must divide ak. The smallest integer multiple of a which is divisible by n is $lcm(a, n) = \frac{an}{\gcd(a,n)}$. Then from $ak = \frac{an}{\gcd(a,n)}$, one deduces $k = \frac{n}{\gcd(a,n)}$.

In our case G is the additive cyclic group $\mathbb{Z}/n\mathbb{Z}$ of order n with generator $\bar{1}$. Then the order of $\bar{x} = x \cdot \bar{1}$ equal to $\frac{n}{\gcd(x,n)}$.

(b) Since $\gcd(185, 1517) = 37$, the order of $\bar{x} = \overline{185}$ in $\mathbb{Z}/1517\mathbb{Z}$ is equal to $\frac{1517}{37} = 41$.

Problem 5. *Verify that $p = 347$ is prime. State Fermat Little Theorem for $p = 347$ and check it for some classes $\bar{x} \in \mathbb{Z}_p^*$.*

Solution. If 347 were not prime, it would be divisible by a prime

$$p \leq \sqrt{347} \leq 19, \qquad p \in \{2, 3, 5, 7, 11, 13, 17, 19\}.$$

This is not the case, hence 347 is prime. FLT says that for every $x \in \mathbb{Z}$ such that $\gcd(x, 347) = 1$, one has

$$x^{346} \equiv 1 \pmod{347}.$$

For example,

$$2^{346} \equiv 1, \qquad 5^{346} \equiv 1, \qquad 13^{346} \equiv 1 \pmod{347}.$$

Problem 6. *A Carmichael number is a composite integer n such that*

$$a^{n-1} \equiv 1, \quad \forall a \in \mathbb{Z}, \quad \textit{with } \gcd(a, n) = 1.$$

Let n be a square free composite integer. Prove that n is a Carmichael number if and only if it has the following property

$$\textit{if } p \textit{ divides } n, \textit{ then } p - 1 \textit{ divides } n - 1.$$

Solution. If n is a square free composite integer, then

$$n = p_1 p_2 \dots p_k,$$

where $p_1, \dots, p_k$ are all distinct primes. In particular $\gcd(p_i, p_j) = 1$, for $i \neq j$. By the Chinese Remainder Theorem, a congruence

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

is equivalent to the system of congruences

$$\begin{cases} a^{n-1} \equiv 1 \pmod{p_1} \\ \qquad \vdots \\ a^{n-1} \equiv 1 \pmod{p_k}. \end{cases}$$

Note that $\gcd(a,n)=1$ if and only if $\gcd(a,p_j)=1$, for all $j=1,\dots,k$. We prove both implications. Suppose first that n is a Carmichael number. Fix j. Since $(\mathbb{Z}/p_j\mathbb{Z})^*$ is cyclic, choose a class $\bar{b}_j$ of order p_j-1 modulo p_j. By the Chinese Remainder Theorem choose an integer a such that

$$a \equiv b_j \pmod{p_j}, \qquad a \equiv 1 \pmod{p_i} \quad (i \neq j).$$

Then $\gcd(a,n)=1$, hence $a^{n-1} \equiv 1 \pmod{n}$ and in particular $b_j^{n-1} \equiv 1 \pmod{p_j}$. Since b_j has order p_j-1, this implies $p_j - 1 \mid n-1$.

Conversely, suppose that $p_j - 1 \mid n-1$ for every j. If $\gcd(a,n)=1$, then $\gcd(a,p_j)=1$ for every j, and Fermat Little Theorem gives $a^{p_j-1} \equiv 1 \pmod{p_j}$. Since $p_j - 1 \mid n-1$, we get $a^{n-1} \equiv 1 \pmod{p_j}$ for every j. By the Chinese Remainder Theorem, $a^{n-1} \equiv 1 \pmod{n}$. Thus n is a Carmichael number.

Problem 7. *Construct your own RSA set of keys N, E, D.*
(N the modulus, E the encrypting key, D the decrypting key).

Solution. Choose primes p and q. Compute $N = p \cdot q$. Choose E with $\gcd(E,(p-1)(q-1))=1$. Compute $D \equiv E^{-1} \pmod{(p-1)(q-1)}$.

Problem 8. *(mini RSA) Mr. White wants to receive encrypted messages and has the RSA set of keys*

$$N = 779, \quad E = 31, \quad D = 511.$$

(a) Check that N, E, D are a good set of keys.
(b) Send the message $m = 11$ to Mr. White after having encrypted it.

Solution. (a) One has $N = 779 = 19 \cdot 41$. Then $\varphi(N) = 18 \cdot 40 = 720$. Since $\gcd(31, 720) = 1$ and from the extended Euclidean algorithm we find

$$31^{-1} \equiv -209 \equiv 511 \pmod{720},$$

the above N, E, D are a good set of keys.
(b) We send to Mr. White $m^E \pmod{N}$:

$$11^{31} \equiv 106 \pmod{779}.$$

Problem 9. *Let $N \in \mathbb{Z}_{>0}$ and let E_1, $E_2 \in \mathbb{Z}_{>0}$ be coprime. Assume that* $\gcd(m, N) = 1$.

(a) Show that you can determine m, knowing

$$m^{E_1} \pmod N \qquad \text{and} \qquad m^{E_2} \pmod N.$$

(b) Let $E_1 = 47$, $E_2 = 53$ and $N = 101$. Find m knowing that

$$m^{E_1} \equiv 28 \pmod{101}, \qquad m^{E_2} \equiv 83 \pmod{101}.$$

Solution. (a) Since $\gcd(E_1, E_2) = 1$, then from the extended Euclidean algorithm we obtain $a, b \in \mathbb{Z}$ such that $aE_1 + bE_2 = 1$. Then, since m is invertible modulo N, negative powers are meaningful and m can be obtained as

$$m \equiv m^{aE_1+bE_2} = (m^{E_1})^a (m^{E_2})^b \pmod N.$$

(b) From $\gcd(47, 53) = 1$, by the extended Euclidean algorithm we obtain $a = -9$ and $b = 8$ such that $-9 \cdot 47 + 8 \cdot 53 = 1$. Then

$$m = (28)^{-9}(83)^8 \equiv 2 \cdot 56 \equiv 11 \pmod{101}.$$

Problem 10. *Determine all the solutions of the equation $\bar{x}^2 = \bar{1}$ in $\mathbb{Z}/11\mathbb{Z}$ and in $\mathbb{Z}/15\mathbb{Z}$.*

Solution. We have that $\bar{x}^2 - \bar{1} = (\bar{x} - \bar{1})(\bar{x} + \bar{1}) = \bar{0}$ in $\mathbb{Z}/11\mathbb{Z}$ if and only if $x^2 - 1 \equiv 0 \pmod p$ if and only if p divides $(x-1)(x+1)$. Since $p = 11$ is prime, this happens if and only if either p divides $(x-1)$ or p divides $(x+1)$. That is if and only if $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$. Hence the only solutions of $\bar{x}^2 - \bar{1} = \bar{0}$ in $\mathbb{Z}/11\mathbb{Z}$ are $\bar{x} = \bar{1}$ and $\bar{x} = \overline{-1}$.

By the Chinese Remainder Theorem, the congruence $x^2 \equiv 1 \pmod{15}$ is equivalent to the system of congruences

$$\begin{cases} x^2 \equiv 1 \pmod 3 \\ x^2 \equiv 1 \pmod 5. \end{cases}$$

Each of the above congruences has 2 solutions, hence the system and the original congruence have 4 solutions. They are

$$x \equiv 1,\ 4,\ 11,\ 14 \pmod{15}.$$

Problem 11. *Let p be a prime. Prove that*

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

Solution. For $p = 2$ the congruence is $1! \equiv 1 \equiv -1 \pmod 2$. Let now $p > 2$ be a prime. Then p is odd and $p-1$ is even. We can interpret the above congruence as the identity

$$\bar{1} \cdot \bar{2} \cdot \ldots \cdot \overline{p-2} \cdot \overline{p-1} = \overline{p-1} \qquad (*)$$

in $(\mathbb{Z}/p\mathbb{Z})^*$. Every class $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^*$ can be paired with its inverse $\bar{x}^{-1} \neq \bar{x}$, except for $\bar{1} = \bar{1}^{-1}$ and $\overline{p-1} = \overline{p-1}^{-1}$. Then the identity (*) holds true and $(p-1)! \equiv -1 \pmod p$, as claimed.

Problem 12. *Let p be a prime.*

(a) Show that if g is a primitive root modulo p, then g^k is a primitive root modulo p if and only if $\gcd(k, p-1) = 1$.

(b) Let $\bar{a}$ and $\bar{b}$ be primitive roots modulo p. Show that $\log_{\bar{a}} \bar{b}$ is invertible modulo $p-1$.

Solution. (a) A primitive root g modulo p is an element of order $p-1$ in the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. Since the order of g^k is equal to $\frac{p-1}{\gcd(k,p-1)}$, one has that g^k is a primitive root modulo p if and only if $\gcd(k, p-1) = 1$.
(b) Since $\bar{a}$ is a primitive root, one can write $\bar{b} = \bar{a}^m$, for some $m \in \mathbb{Z}/(p-1)\mathbb{Z}$. By definition, $m = \log_{\bar{a}} \bar{b}$. By part (a) of the exercise, $\bar{a}^m$ is a primitive root if and only if $\gcd(m, p-1) = 1$. It follows that $\log_{\bar{a}} \bar{b}$ is invertible modulo $p-1$.

Problem 13. *Find a primitive root modulo $p = 47$.*

Solution. We use the criterion which says that *a is a primitive root modulo p if and only if for every prime divisor d of $p-1$ one has*

$$a^{(p-1)/d} \not\equiv 1 \pmod{p}. \qquad (**)$$

In this case, $p-1 = 46 = 2 \cdot 23$. Hence we have to check the two conditions

$$a^2 \not\equiv 1 \pmod{47}, \qquad a^{23} \not\equiv 1 \pmod{47}.$$

• Let's try $a = 2$:

$$2^2 \not\equiv 1 \pmod{47}, \qquad 2^{23} \equiv 1 \pmod{47}.$$

Conclusion $a = 2$ is not a primitive root modulo 47.

• Let's try $a = 3$:

$$3^2 \not\equiv 1 \pmod{47}, \qquad 3^{23} \equiv 1 \pmod{47}.$$

Conclusion $a = 3$ is not a primitive root modulo 47.

• Let's try $a = 5$:

$$5^2 \not\equiv 1 \pmod{47}, \qquad 5^{23} \equiv 46 \not\equiv 1 \pmod{47}.$$

Conclusion $a = 5$ is a primitive root modulo 47.

Problem 14. *Compute the orders of* $\bar{2}$ *in* $\mathbb{Z}/35\mathbb{Z}$ *and in* $(\mathbb{Z}/35\mathbb{Z})^*$.

Solution. • The element $\bar{1}$ is a generator of additive group $\mathbb{Z}/35\mathbb{Z}$. In particular $\bar{1}$ has order 35. Since $\gcd(2, 35) = 1$, then also the element $\bar{2} = 2 \cdot \bar{1}$ has order 35.

• Recall that

$$(\mathbb{Z}/35\mathbb{Z})^* \to (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^*, \quad \bar{2} \pmod{35} \mapsto (\bar{2} \pmod{5},\ \bar{2} \pmod{7})$$

is a group isomorphism, that $(\mathbb{Z}/5\mathbb{Z})^*$ is a cyclic group of order 4 and that $(\mathbb{Z}/7\mathbb{Z})^*$ is a cyclic group of order 6. It follows that the order of $\bar{2}$ in $(\mathbb{Z}/35\mathbb{Z})^*$ is $\leq lcm(4, 6) = 12$.

More precisely, the order of $\bar{2}$ is the lowest common multiple of the order of $\bar{2}$ in $(\mathbb{Z}/5\mathbb{Z})^*$ and the order of $\bar{2}$ in $(\mathbb{Z}/7\mathbb{Z})^*$. It is easy to check that the order of $\bar{2}$ in $(\mathbb{Z}/5\mathbb{Z})^*$ is 4 and that the order of $\bar{2}$ in $(\mathbb{Z}/7\mathbb{Z})^*$ is 3. Hence the order of $\bar{2}$ in $(\mathbb{Z}/35\mathbb{Z})^*$ is $12 = lcm(4, 3)$.

Problem 15. *a) Prove that* 2 *is a primitive root modulo* $11, 13, 19$*, but not modulo* 17.

b) Prove that $\log_{\bar{2}} \bar{3}$ *does not exist in* $(\mathbb{Z}/17\mathbb{Z})^*$.

c) Compute $\log_{\bar{2}} \bar{3}$ *in* $(\mathbb{Z}/11\mathbb{Z})^*$, $(\mathbb{Z}/13\mathbb{Z})^*$, *and* $(\mathbb{Z}/19\mathbb{Z})^*$.

Solution. (a) We use the criterion (**).

• $p = 11$, $p - 1 = 10 = 2 \cdot 5$

$$2^2 \not\equiv 1 \mod 11, \qquad 2^5 \equiv -1 \not\equiv 1 \mod 11.$$

• $p = 13$, $p - 1 = 12 = 2^2 \cdot 3$

$$2^4 \equiv 3 \not\equiv 1 \mod 13, \qquad 2^6 \equiv 12 \not\equiv 1 \mod 13.$$

• $p = 19$, $p - 1 = 18 = 2 \cdot 3^3$

$$2^6 \equiv 7 \not\equiv 1 \mod 19, \qquad 2^9 \equiv 18 \not\equiv 1 \mod 19.$$

Conclusion: 2 is a primitive root modulo $11, 13, 19$.

• $p = 17$, $p - 1 = 16 = 2^4$

$$2^8 \equiv 1 \pmod{17}.$$

Conclusion 2 is not a primitive root modulo 17.

(b) We check that in $(\mathbb{Z}/17\mathbb{Z})^*$

$$\bar{2}^m \neq \bar{3}, \quad \forall m \in \mathbb{Z}.$$

In fact the distinct powers of $\bar{2}$ are

$$\bar{2}, \quad \bar{2}^2 = \bar{4}, \quad \bar{2}^3 = \bar{8}, \quad \bar{2}^4 = \overline{16}, \quad \bar{2}^5 = \overline{15}, \quad \bar{2}^6 = \overline{13}, \quad \bar{2}^7 = \bar{9}, \quad \bar{2}^8 = \bar{1}.$$

(from now on they repeat cyclically...)

(c) We just try powers of $\bar{2}$ in $(\mathbb{Z}/11\mathbb{Z})^*$, $(\mathbb{Z}/13\mathbb{Z})^*$, and $(\mathbb{Z}/19\mathbb{Z})^*$, as we have not learned any algorithm to do it...

• $p = 11$

$$\bar{2}, \quad \bar{2}^2 = \bar{4}, \quad \bar{2}^3 = \bar{8}, \quad \bar{2}^4 = \bar{5}, \quad \bar{2}^5 = \overline{10}, \quad \bar{2}^6 = \bar{9}, \quad \bar{2}^7 = \bar{7}, \quad \bar{2}^8 = \bar{3}.$$

Conclusion: $\log_{\bar{2}} \bar{3} = 8$ in $(\mathbb{Z}/11\mathbb{Z})^*$.

• $p = 13$

$$\bar{2}, \quad \bar{2}^2 = \bar{4}, \quad \bar{2}^3 = \bar{8}, \bar{2}^4 = \bar{3}.$$

Conclusion: $\log_{\bar{2}} \bar{3} = 4$ in $(\mathbb{Z}/13\mathbb{Z})^*$.

• $p = 19$

$$\bar{2}, \quad \bar{2}^2 = \bar{4}, \quad \bar{2}^3 = \bar{8}, \quad \bar{2}^4 = \overline{16}, \quad \bar{2}^5 = \overline{13}, \quad \bar{2}^6 = \overline{7}, \quad \bar{2}^8 = \overline{9}, \quad \bar{2}^{10} = \overline{17}, \quad \bar{2}^{11} = \overline{15},$$

$$\bar{2}^{12} = \overline{11}, \quad \bar{2}^{13} = \overline{3}.$$

Conclusion: $\log_{\bar{2}} \bar{3} = 13$ in $(\mathbb{Z}/19\mathbb{Z})^*$.

Problem 16. *Suppose we know that $p = 2^{16} + 1 = 65537$ is a prime and that 3 is a primitive root modulo p.*

a) How many primitive roots mod p are there?

b) What is the order of $\bar{2}$ in $(\mathbb{Z}/p\mathbb{Z})^*$? is 2 a primitive root modulo p?

c) What is the order of $\bar{9}$ in $(\mathbb{Z}/p\mathbb{Z})^*$? is 9 a primitive root modulo p?

d) Without any calculations, write down at least five different primitive roots modulo p.

e) Show that $\log_{\bar{3}} \bar{2}$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiple of 2^{11}.

f) Show that a is a primitive root modulo p if and only if the equation $x^2 - a = 0$ has no solutions in $\mathbb{Z}/p\mathbb{Z}$.

Solution. (a) If $p = 2^{16} + 1$, then $p - 1 = 2^{16}$. In $(\mathbb{Z}/p\mathbb{Z})^*$ there are

$$\varphi(p-1) = 2^{16} - 2^{15} = 2^{15}$$

primitive roots.

(b) The group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1 = 2^{16}$. Then the order $\bar{2}$, which is a divisor of 2^{16}, is equal to 2^a, for some positive integer a. From

$$2^{16} + 1 \equiv 0 \pmod{p} \quad \Leftrightarrow \quad 2^{16} \equiv -1 \pmod{p},$$

we obtain

$$2^{32} \equiv 1 \pmod{p}.$$

We claim that the order of $\bar{2}$ *is indeed* $32 = 2^5$.
This follows from the fact that all the powers

$$\bar{2}^2 = \bar{4}, \qquad \bar{2}^{2^2} = \bar{2}^4 = \overline{16}, \qquad \bar{2}^{2^3} = \bar{2}^8 = \overline{256}, \qquad \bar{2}^{2^4} = \bar{2}^{16} = \overline{-1}$$

are different from $\bar{1}$ in $(\mathbb{Z}/p\mathbb{Z})^*$.

(c) We know that $\bar{3}$ is a primitive root modulo p, i.e. it is an element of order 2^{16}. Since $\gcd(2, 2^{16}) = 2 \neq 1$, the order $\bar{9} = \bar{3}^2$ is $2^{15} < 2^{16}$. In particular $\bar{9}$ is not a primitive root modulo p.

(d) If $\bar{3}$ is a primitive root in $(\mathbb{Z}/p\mathbb{Z})^*$, then all the other ones are

$$\bar{3}^k, \qquad \text{with } k \in \mathbb{Z},\ \gcd(k, 2^{16}) = 1, \text{ i.e. with } k \text{ odd.}$$

For example

$$\bar{3}^3, \quad \bar{3}^5, \quad \bar{3}^7, \quad \bar{3}^9, \quad \bar{3}^{11}.$$

(e) Since $\bar{3}$ is a primitive root, we can write

$$\bar{2} = \bar{3}^m, \qquad \text{where } m = \log_{\bar{3}} \bar{2}.$$

We have (see the solution of Exercise 4(a))

$$2^5 = ord(\bar{2}) = ord(\bar{3}^m) = \frac{p-1}{\gcd(m, p-1)} = \frac{2^{16}}{\gcd(m, 2^{16})}.$$

We conclude that $\gcd(m, 2^{16}) = 2^{11}$ and therefore $m = \log_{\bar{3}} \bar{2}$ is an integer multiple of 2^{11}.

(f) Showing that a is a primitive root modulo p if and only if the equation $x^2 - a = 0$ has no solutions in $\mathbb{Z}/p\mathbb{Z}$ is equivalent to showing that

a is a primitive root modulo p if and only if a is not a square modulo p.

Proof. Let g be a primitive root modulo p. Every non-zero class can be written uniquely as g^r. Moreover g^r is a square if and only if r is even: indeed the squares are $(g^s)^2 = g^{2s}$.

If a is a primitive root, say $a = g^r$, then

$$2^{16} = ord(a) = ord(g^r) = \frac{2^{16}}{\gcd(r, 2^{16})},$$

so $\gcd(r, 2^{16}) = 1$ and therefore r is odd. Thus a is not a square. Conversely, if a is not a square, then $a = g^r$ with r odd. Hence $\gcd(r, 2^{16}) = 1$, and

$$ord(a) = ord(g^r) = \frac{2^{16}}{\gcd(r, 2^{16})} = 2^{16}.$$

Therefore a is a primitive root modulo p.

Problem 17. *Mr. White and Mr. Red agree on the prime $p = 151$ and on the primitive root $g = 6$ modulo p. The secret key of Mr. White is $W = 111$, the secret key of Mr. Red is $R = 76$. After performing a Diffie-Hellman protocol, what is the secret key that they will share?*

Solution. Mr. White computes and sends to Mr. Red $6^{111} \equiv 26 \pmod{151}$. Mr. Red computes $(26)^{76} \pmod{151}$.

Mr. Red computes and sends to Mr. White $6^{76} \equiv 145 \pmod{151}$. Mr. White computes $(145)^{111} \pmod{151}$. At the end they both have the secret key

$$(6^{111})^{76} \equiv (6^{76})^{111} \equiv 6^{8436} \equiv 125 \pmod{151}.$$

Remark. Suppose that a spy intercepts the numbers 26 and 145 travelling from one user to the other: he cannot obtain the secret key unless he can solve the discrete logarithm problem in $(\mathbb{Z}/151\mathbb{Z})^*$. (of course in the real world the prime number p is much larger than 151 !!!).