MTH6115 Cryptography

Solutions 8

---

1 Consider the numbers $\{ g^k \mid 0 \leqslant k < p-1 \}$. They are pairwise distinct mod p, because if $g^k \equiv g^l \pmod p$ for some $0 \leqslant k < l < p-1$, then we would have $g^{l-k} \equiv 1 \pmod p$, contradicting the fact that p is a primitive root. So, the set $\{ g^k \mid 0 \leqslant k < p-1 \}$ contains $p-1$ pairwise distinct nonzero residue classes mod p. Since we have precisely $p-1$ nonzero residue classes mod p, the above set should represent all of them.

2 First suppose that l is coprime to $\varphi(n)$. Then, there exist k such that $kl \equiv 1 \pmod n$. Now, if $a^m \equiv 1 \pmod n$ then, by Lemma A, $(a^l)^m \equiv 1 \pmod n$. Conversely, $(a^l)^m \equiv 1 \pmod n$ implies, again by Lemma A, that $(a^{kl})^m = ((a^l)^m)^k \equiv 1 \pmod n$. It follows that the smallest such m for a coincides with the smallest such m for a^l, hence a and a^l have the same order mod n.

To prove the reverse implication, let $\gcd(l, \varphi(n)) = d > 1$. Let $m = \mathrm{ord}_n(a)$. Then, $(a^l)^{m/d} = (a^m)^{l/d} \equiv 1 \pmod n$, by Lemma A. So, $\mathrm{ord}_n(a^l) \leq m/d$. (Exercise: show that in fact $\mathrm{ord}_n(a^l) = m/d$.)

3 a) By Problem 1 every residue class mod p is of the form g^k for some $0 \leqslant k < p-1$. By Problem 2, when k is coprime to $p-1$ the order of g^k is equal to the order of g, so g^k is a primitive root. If k is not coprime to $p-1$, say $\gcd(k, p-1) = d > 1$, then $(g^k)^{\frac{p-1}{d}} \equiv (g^{p-1})^{\frac{k}{d}} \equiv 1 \pmod p$, so the order of g^k is at most $\frac{p-1}{d}$. Hence, g^k is not a primitive root. So, the set of primitive roots in $\mathbb{Z}_p$ is precisely $\{ g^k \mid 0 \leqslant k < p-1,\ \gcd(k, p-1) = 1 \}$.

b) We have seen in the supplementary notes that 2 is a primitive root mod 19. The numbers $0 < k < 19 - 1$ coprime to 18 are $1, 5, 7, 11, 13, 17$. So, the primitive roots mod 19 are

$$\{2,\ 2^5 \equiv 13,\ 2^7 \equiv 14,\ 2^{11} \equiv 15,\ 2^{13} \equiv 3,\ 2^{17} \equiv 10 \pmod{19}\},$$

that is

$$\{2, 3, 10, 13, 14, 15\}.$$

4 a) First we find the order of 2 mod 41. The order of any number mod 41 divides 40, so it is one of the following numbers: $1, 2, 4, 5, 8, 10, 20, 40$. The first three clearly don't work. We have $2^5 \equiv 32 \equiv -9 \pmod{41}$ which doesn't work either, but $2^{10} \equiv (-9)^2 \equiv 81 \equiv -1 \pmod{41}$ is pretty close. In fact, this implies that the order of 2 mod 41 is 20. We immediately deduce that the order of $4 = 2^2$ mod 41 is 10 and the order of $8 = 2^3$ mod 41 is 20 (because $\gcd(3, 40) = 1$).

Let k be the order of 7 mod 41. Note that $7^2 \equiv 8 \pmod{41}$. Since $8^k \equiv 7^{2k} \equiv 1 \pmod{41}$, and since the order of 8 is 20, we must have $20|k$. If $k = 20$, we would have $8^{10} = 7^{20} \equiv 1 \pmod{41}$ which is not possible. Therefore, the order of 7 mod 41 is 40. That is, 7 is a primitive root mod 41.

b) The order of any number mod 23 divides 22, so it is one of the following numbers: $1, 2, 11, 22$. The order of 5 is not 1, and is not 2 either because $5^2 = 25 \equiv 2 \pmod{23}$. We try 11. We have $5^{11} \equiv (5)(5^2)^5 \equiv (5)(2)^5 \equiv (5)(32) \equiv (5)(9) \equiv -1$. So the order of 5 is 22, that is, 5 is a primitive root mod 23.

To find the order of 18, note that $18 \equiv -5 \pmod{23}$. So we can use the above calculations, being careful about the signs. We see that 11 works, that is, the order of 18 mod 23 is 11.

5 (a) We have $107 - 1 = 106 = 2 \cdot 53$. Clearly, $2^2 = 4 \not\equiv 1 \pmod{107}$. We now calculate $2^{53} \pmod{107}$ as follows:

$$2^7 = 128 \equiv 21, \quad 2^{14} \equiv 21^2 \equiv 13, \quad 2^{28} \equiv 13^2 \equiv 62 \pmod{107}$$
$$2^{27} \equiv 31, \quad 2^{54} \equiv 105 \equiv -2 \pmod{107}$$

Dividing by 2, we find that $2^{53} \equiv -1 \pmod{107}$. Hence, 2 is a primitive root modulo 107.

(b) We saw above that $2^7 \equiv 21 \pmod{107}$.

$2^{14} \equiv 13 \pmod{107}$, so $2^{15} \equiv 26 \equiv -81 \pmod{107}$. So $81 \equiv 2^{53} \cdot 2^{15} = 2^{68} \pmod{107}$. (Can we conclude that $3 \equiv 2^{68/4} \equiv 2^{17} \pmod{107}$?)

Notice that $4 \cdot 27 = 108 \equiv 1 \pmod{107}$, so $27 \equiv 2^{-2} \equiv 2^{104} \pmod{107}$. (We used Fermat's theorem.)

By Fermat, $27 \equiv 2^{104} \equiv 2^{210} \pmod{106}$. So $3 \equiv 2^{210/3} \equiv 2^{70} \pmod{107}$. (Why can we do this?)

We know 21 and 3, so we calculate $7 \equiv 2^{7-70} \equiv 2^{-63} \equiv 2^{43} \pmod{107}$.

$14 = 2 \cdot 7 \equiv 2^1 \cdot 2^{43} = 2^{44} \pmod{107}$.

(c) By part (b), we know that $14 \equiv 2^{44} \pmod{107}$, so $x = 2^{11} \equiv 15 \pmod{107}$ is a solution. The other solution is $x = -15 \equiv 92 \pmod{107}$.

6 (a) We have $131 - 1 = 130 = 2 \cdot 5 \cdot 13$. In order to show 2 is a primitive root modulo 131 we must therefore calculate 2^{130}, $2^{65} = 2^{130/2}$, $2^{26} = 2^{130/5}$ and $2^{10} = 2^{130/13}$ modulo 131, where the first of these is required to be congruent to 1 modulo 131, and the others must not be congruent to 1 modulo 131. Calculating modulo 131 we have:

$$2^3 = 8, \quad 2^5 = 32, \quad 2^{10} = 32^2 = 1024 \equiv 107 \equiv -24,$$
$$2^{13} \equiv 8 \cdot (-24) = -192 \equiv -61 \not\equiv 1, \quad 2^{26} \equiv 61^2 = 3721 \equiv 53 \not\equiv 1,$$
$$2^{52} = (2^{26})^2 \equiv 53^2 = 2809 \equiv 58, \quad 2^{65} \equiv (-61) \cdot 58 = -3538 \equiv -1 \not\equiv 1$$

Thus $2^{130} \equiv (-1)^2 = 1 \pmod{131}$, which together with the above proves that 2 is a primitive root modulo 131.

(b) There are several useful tricks to find a without the need to do much clacu- lations. You will see a few of these trick in the following. You have seen a few in the previous problem as well.

First note that, since 2 is a primitive root, we have $2^{65} \equiv -1 \pmod{131}$, as we saw above.

$123 \equiv -8 \equiv 2^{65} \cdot 2^3 \equiv 2^{68} \pmod{131}$.

$101 \equiv 232 = 4 \cdot 58 \equiv 2^2 \cdot 2^{52} \equiv 2^{54} \pmod{131}$.

$2^7 \equiv 128 \equiv -3 \pmod{131}$, so $3 \equiv 2^{65} \cdot 2^7 \equiv 2^{72} \pmod{131}$.

$81 = 3^4 \equiv (2^{72})^4 \equiv 2^{28} \pmod{131}$.

$3 \cdot 41 = 123 \equiv 2^{68}$, so $41 \equiv 2^{68-72} \equiv 2^{-4} \equiv 2^{130-4} \equiv 2^{126} \pmod{131}$.

For $a = 15$, note that $9 \cdot 15 = 135 \equiv 4 \pmod{131}$. Since $9 = 3^2 \equiv 2^{2 \cdot 72} = 2^{144} \equiv 2^{14} \pmod{131}$, we have $15 \equiv 2^{2-14} \equiv 2^{-12} \equiv 2^{118} \pmod{131}$.

(c) We have $\lambda(10000) = \operatorname{lcm}\{\lambda(2^4), \lambda(5^4)\} = \operatorname{lcm}\{4, 5^3(4)\} = 500$, so $3^{500} \equiv 1 \pmod{10000}$. Therefore,

$$3^{1005} \equiv (3^{1000})(3^5) \equiv (1)(243) \pmod{10000}.$$

So, the last four digits are 0243.