

Homework Set 9

Problem 1

Example 11. List all primitive roots modulo 14.

Solution. Since $\phi(14) = \phi(2)\phi(7) = 6$, the possible orders of residues modulo 14 are 1, 2, 3, 6. Residues with order 6 are primitive roots. Our strategy is to find one primitive root and to use that to compute all primitive roots. There is no good way of finding the first primitive root. We will just try the residues 3, 5, ... (we are skipping 2 because it is not invertible modulo 14).

We compute the order of 3 (mod 14):

Since $3^2 = 9 \not\equiv 1$, $3^3 \equiv -1 \not\equiv 1 \pmod{14}$, we find that 3 has order 6. Hence, 3 is a primitive root.

All other invertible residues are of the form 3^x with $x = 0, 1, 2, \dots, 5$ (note that $5 = \phi(14) - 1$).

Recall that the order of $3^x \pmod{14}$ is $\frac{6}{\gcd(6, x)}$.

Hence, 3^x is a primitive root if and only if $\gcd(6, x) = 1$, which yields $x = 1, 5$.

In conclusion, the primitive roots modulo 14 are $3^1 = 3, 3^5 \equiv 5$.

Example 12. List all primitive roots modulo 22.

Solution. We proceed as in the previous example:

- Since $\phi(22) = 10$, the possible orders of residues modulo 22 are 1, 2, 5, 10.
- We find one primitive root by trying residues 3, 5, ... (2 is out because it is not invertible modulo 22).
 $3^2 \not\equiv 1$ but $3^5 \equiv 1 \pmod{22}$, so 3 is not a primitive root modulo 22.
 $5^2 \not\equiv 1$ but $5^5 \equiv 1 \pmod{22}$, so 5 is not a primitive root modulo 22.
 $7^2 \not\equiv 1$, $7^5 \equiv -1 \not\equiv 1 \pmod{22}$, so 7 is a primitive root modulo 22.
- $7^x \pmod{22}$ has order $\frac{10}{\gcd(10, x)}$. We have $\gcd(10, x) = 1$ for $x = 1, 3, 7, 9$.
- Hence, the primitive roots modulo 22 are $7^1 = 7, 7^3 \equiv 13, 7^7 \equiv 17, 7^9 \equiv 19$.

Problem 2

Example 13. 3 is a primitive root modulo 98. For which x is 3^x a primitive root modulo 98?

Solution. Since it is a primitive root, 3 has order $\phi(98) = \phi(2)\phi(7^2) = (2-1)(7^2-7^1) = 42$.

$3^x \pmod{98}$ has order $\frac{42}{\gcd(42, x)}$. Hence 3^x a primitive root modulo 98 if and only if $\gcd(42, x) = 1$.

Those x are 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

Comment. Note that these are $\phi(\phi(98)) = \phi(42) = 12$ primitive roots.

Problem 3

Example 14. What is the number of primitive roots modulo 29?

Solution. $\phi(\phi(29)) = \phi(28) = \phi(4)\phi(7) = (4-2) \cdot 6 = 12$

Problem 4

Example 15. Bob's public RSA key is $N = 77$, $e = 49$. Encrypt the message $m = 38$ for sending it to Bob.

Solution. The ciphertext is $c = m^e \pmod{N}$. Here, $c \equiv 38^{49} \equiv 31 \pmod{77}$. Hence, $c = 31$.

Here, we skipped over the computation of $38^{49} \pmod{77}$ because we discussed these earlier. Your options include:

- Doing the computation by hand using binary exponentiation (and a calculator for support):
 $38^2 \equiv 58$, $38^4 \equiv 53$, $38^8 \equiv 37$, $38^{16} \equiv 60$, $38^{32} \equiv 58 \pmod{77}$
 Since $49 = 32 + 16 + 1$, we have $38^{49} = 38^{32} \cdot 38^{16} \cdot 38 \equiv 58 \cdot 60 \cdot 38 \equiv 31 \pmod{77}$.
- If you are comfortable with binary exponentiation, you may use Sage to do the computation:

```
>>> power_mod(38, 49, 77)
```

```
31
```

- If you insisted on doing things by hand and without any support by a calculator, you could use the Chinese Remainder Theorem to work with smaller numbers:

$$38^{49} \equiv 3^{49} \equiv 3^1 = 3 \pmod{7}$$

[we used little Fermat to reduce the exponent]

$$38^{49} \equiv 5^{49} \equiv 5^{-1} \equiv -2 \pmod{11}$$

[note how we preferred 5^{-1} over 5^9]

$$\text{Therefore, } 38^{49} \equiv 3 \cdot \underbrace{11 \cdot 11^{-1}}_2 - 2 \cdot 7 \cdot \underbrace{7^{-1}}_{-3} \equiv 66 + 42 \equiv 31 \pmod{77}.$$

However, notice that we used the fact that $77 = 7 \cdot 11$. In practice, Alice cannot factor N (if she could, then she could easily obtain Bob's private key) so we wouldn't be able to proceed this way. However, when Bob decrypts he could (and in practice often does!) use the Chinese Remainder Theorem.

Problem 5

Example 16. Bob's public RSA key is $N = 35$, $e = 17$. Determine Bob's secret key.

Solution. The private key is $d = e^{-1} \pmod{\phi(N)}$. Here, since $\phi(35) = 4 \cdot 6 = 24$, the key is $d = 17^{-1} \pmod{24}$.

We compute $17^{-1} \pmod{24}$ using the extended Euclidean algorithm (or, if you are comfortable with that, using Sage):

$$\begin{aligned} 24 &= 1 \cdot 17 + 7 \\ 17 &= 2 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (17 - 2 \cdot 7) = 5 \cdot 7 - 2 \cdot 17 = 5 \cdot (24 - 17) - 2 \cdot 17 = 5 \cdot 24 - 7 \cdot 17.$$

Hence, $17^{-1} \equiv -7 \equiv 17 \pmod{24}$ and, so, $d = 17$.

Alternatively. If you are comfortable with applying the extended Euclidean algorithm to compute inverses, you can alternatively use Sage:

```
>>> inverse_mod(17, 24)
```

```
17
```

Comment. Actually, as will be discussed in class, $\phi(N) = (p - 1)(q - 1) = 4 \cdot 6$ can be replaced with $\text{lcm}(p - 1, q - 1) = \text{lcm}(4, 6) = 12$. It follows that the pair $(e, d) = (17, 17)$ is equivalent to the pair $(e, d) = (5, 5)$.

Problem 6

Example 17. Bob's public RSA key is $N = 55$, $e = 31$. You intercept the encrypted message $c = 7$ from Alice to Bob. Break the cipher and determine the plaintext.

Solution. First, as in the previous problem, we determine Bob's secret key: $d = e^{-1} \pmod{\phi(N)}$. Here, since $\phi(55) = 4 \cdot 10 = 40$, the key is $d = 31^{-1} \equiv 31 \pmod{40}$. [It's a coincidence due to small numbers that $d = e$ again.] Finally, we need to compute $m = c^d \pmod{N}$, that is, $m = 7^{31} \equiv 18 \pmod{55}$.

Problem 7

Example 18. Bob randomly generated $N = 119$ for his public RSA key. What is the smallest possible choice for e ?

Solution. Recall that e must be invertible modulo $\phi(N) = \phi(7)\phi(17) = 6 \cdot 16$. Hence, $e = 2, 3, 4$ are not allowed. Therefore, the smallest possible choice for e is $e = 5$.

Problem 8

Example 19. Find x such that $8 \equiv 3^x \pmod{19}$.

Solution. We proceed by brute-force and just go through the possibilities:

$$3^2 = 9, 3^3 \equiv 8 \pmod{19}$$

Hence, $x = 3$.

As the next example shows, sometimes we might have to look for a while before finding the discrete logarithm.

[However, I have programmed the homework problem so that you will not have to search for long.]

Example 20. Find x such that $4 \equiv 3^x \pmod{19}$.

Solution. We proceed by brute-force and just go through the possibilities:

$$3^2 = 9, 3^3 \equiv 8, 3^4 \equiv 8 \cdot 3 \equiv 5, 3^5 \equiv 5 \cdot 3 \equiv -4, 3^6 \equiv -4 \cdot 3 \equiv 7, 3^7 \equiv 7 \cdot 3 \equiv 2, 3^8 \equiv 2 \cdot 3 \equiv 6, 3^9 \equiv 6 \cdot 3 \equiv -1, 3^{10} \equiv -1 \cdot 3 \equiv -3, 3^{11} \equiv -3 \cdot 3 \equiv -9, 3^{12} \equiv -9 \cdot 3 \equiv -8, 3^{13} \equiv -8 \cdot 3 \equiv -5, 3^{14} \equiv -5 \cdot 3 \equiv 4 \pmod{19}$$

Hence, $x = 14$.

Comment. As a shortcut, when we observed $3^7 \equiv 2 \pmod{19}$, we could have concluded that $4 = 2^2 \equiv 3^{7 \cdot 2} = 3^{14} \pmod{19}$ so that $x = 14$.

Problem 9

Example 21. Alice and Bob select $p = 29$ and $g = 8$ for a Diffie-Hellman key exchange. Alice sends 13 to Bob, and Bob sends 26 to Alice. What is their shared secret?

Solution. If Alice's secret is y and Bob's secret is x , then $8^y \equiv 13$ and $8^x \equiv 26 \pmod{29}$.

We compute $8^2, 8^3, \dots \pmod{29}$ until we find either 13 or 26:

$$8^2 \equiv 6, 8^3 \equiv 6 \cdot 8 \equiv -10, 8^4 \equiv -10 \cdot 8 \equiv 7, 8^5 \equiv 7 \cdot 8 \equiv -2, 8^6 \equiv -2 \cdot 8 \equiv 13 \pmod{29}.$$

Hence, Alice's secret is $y = 6$. The shared secret is $(8^x)^y \equiv 26^6 \equiv 4 \pmod{29}$.