# Homework Set 8 (Lecture 26)

## Problem 1

**Example 10.** 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 $3, 5, \ldots$ (we are skipping $2$ because it is not invertible modulo $14$).

We compute the order of $3 \pmod{14}$:

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 $x = 0, 1, 2, \ldots, 5$ (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 11.** 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 $3, 5, \ldots$ ($2$ 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 12.** 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 3

**Example 13.** 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 exponentation (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 exponentation, 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 $5^9$]
  Therefore, $38^{49} \equiv 3 \cdot 11 \cdot \underbrace{11^{-1}_{\bmod 7}}_{2} - 2 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 11}}_{-3} \equiv 66 + 42 \equiv 31 \pmod{77}$.
  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 4

**Example 14.** 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):

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

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

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

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 $\operatorname{lcm}(p-1, q-1) = \operatorname{lcm}(4, 6) = 12$. It follows that the pair $(e, d) = (17, 17)$ is equivalent to the pair $(e, d) = (5, 5)$.

## Problem 5

**Example 15.** 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, $m = 7^{31} \equiv 18 \pmod{55}$.