Sixth Exercise Session: 4/5

Themes: Number theory, Group theory (optional)

Relevant Chapters: Vol.2: 2 (optional), 3.2; Suppl4.pdf

1. Compute $5^{2022} \pmod{23}$
(i) using Fermat
(ii) by repeated squaring.

2. Determine all the primitive roots modulo 23.

3. Compute $1997^{1997} \pmod{132}$ and $1994^{1994} \pmod{132}$.

4. (Övning 3.34 i Vol. 2) Du har uppsnappat det krypterade budskapet 444, från en person vars offentliga nyckel är $e = 797$ och $n = 1961$. Du har också lyckats spionera fram att $q = 53$. Dekryptera budskapet !

5. Prove Tom Hanks' Volleyball's Theorem (a.k.a. Wilson's Theorem):

If p is a prime, then $(p-1)! \equiv -1$ (mod p).

Solutions

1. (i) By Fermat's Theorem (23 is prime and 5 isn't a multiple of 23), $5^{22} \equiv 1 \pmod{23}$. Now $2022 = 92 \cdot 22 - 2$, thus

$$5^{2022} \equiv (5^{22})^{92} \cdot 5^{-2} \equiv 1^{92} \cdot (5^2)^{-1} \equiv 25^{-1} \equiv 2^{-1} \equiv 12 \pmod{23}.$$

(ii) *Step 1:* Write the power in base 2:

$$\begin{aligned} 2022 &= 2 \cdot 1011 + 0, \\ 1011 &= 2 \cdot 505 + 1, \\ 505 &= 2 \cdot 252 + 1, \\ 252 &= 2 \cdot 126 + 0, \\ 126 &= 2 \cdot 63 + 0, \\ 63 &= 2 \cdot 31 + 1, \\ 31 &= 2 \cdot 15 + 1, \\ 15 &= 2 \cdot 7 + 1, \\ 7 &= 2 \cdot 3 + 1, \\ 3 &= 2 \cdot 1 + 1, \\ 1 &= 2 \cdot 0 + 1. \end{aligned}$$

The sequence of remainders, read backwards, gives the base-2 representation of the number:

$$(2022)_2 = 11111100110.$$

In other words,

$$2022 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^2 + 2^1. \tag{1}$$

Step 2: Repeated squaring. Set $x_0 = 5^{2^0} \equiv 5^1 \equiv 5 \pmod{23}$ and compute recursively

$$x_i \equiv x_{i-1}^2 \equiv 5^{2^i} \pmod{23}, \quad \text{up to } i = 10.$$

Just do it:

$$\begin{aligned} x_1 \equiv 5^2 \equiv 25 \equiv 2, \quad x_2 \equiv 2^2 \equiv 4, \\ x_3 \equiv 4^2 \equiv 16 \equiv -7, \quad x_4 \equiv (-7)^2 \equiv 49 \equiv 3, \\ x_5 \equiv 3^2 \equiv 9, \quad x_6 \equiv 9^2 \equiv 81 \equiv 12, \\ x_7 \equiv 12^2 \equiv 144 \equiv 6, \quad x_8 \equiv 6^2 \equiv 36 \equiv -10, \\ x_9 \equiv (-10)^2 \equiv 100 \equiv 8, \quad x_{10} \equiv 8^2 \equiv 64 \equiv -5. \end{aligned}$$

Step 3: From (1) we have that

$$5^{2022} = 5^{2^{10}+2^9+2^8+2^7+2^6+2^5+2^2+2^1} = 5^{2^{10}} \cdot 5^{2^9} \cdot 5^{2^8} \cdot 5^{2^7} \cdot 5^{2^6} \cdot 5^{2^5} \cdot 5^{2^2} \cdot 5^{2^1} \equiv x_{10}\, x_9\, x_8\, x_7\, x_6\, x_5\, x_2\, x_1 \pmod{23}.$$

We multiply (mod 23), two at a time, to keep all numbers below 23^2. Thus,

$$\begin{aligned} x_{10} \cdot x_9 &\equiv -5 \cdot 8 \equiv -40 \equiv 6, \\ 6 \cdot x_8 &\equiv 6 \cdot (-10) \equiv -60 \equiv 9, \\ 9 \cdot x_7 &\equiv 9 \cdot 6 \equiv 54 \equiv 8, \\ 8 \cdot x_6 &\equiv 8 \cdot 12 \equiv 96 \equiv 4, \\ 4 \cdot x_5 &\equiv 4 \cdot 9 \equiv 36 \equiv 13, \\ 13 \cdot x_2 &\equiv 13 \cdot 4 \equiv 52 \equiv 6, \\ 6 \cdot x_1 &\equiv 6 \cdot 2 \equiv 12. \end{aligned}$$

Thus $5^{2022} \equiv 12 \pmod{23}$, v.s.v.

2. By the proof of Euler's theorem, the order of any element $a \in \mathbb{Z}_n^\times$ must be a divisor of $\phi(n)$. So a will be a primitive root mod n if and only if $a^k \not\equiv 1 \pmod{n}$ for every *proper divisor* k of $\phi(n)$. This simplifies computations as we search for a primitive root.

In our example, $n = 23$, $\phi(n) = 22 = 2 \cdot 11$, so $a \in \{2, 3, \ldots, 22\}$ will be a primitive root (mod 23) if and only if neither a^2 nor a^{11} is congruent to 1 (mod 23). Now we just search.

Test $a = 2$: $2^2 = 4 \not\equiv 1$, o.k. But $2^{11} = (2^5)^2 \cdot 2^1 \equiv 9^2 \cdot 2 \equiv 12 \cdot 2 \equiv 1$, helvete !

Test $a = 3$*:* $3^2 = 9 \not\equiv 1$, o.k. But $3^{11} = (3^3)^3 \cdot 3^2 \equiv 4^3 \cdot 9 \equiv (-5) \cdot 9 \equiv -45 \equiv 1$, duh !

No point testing $a = 4$ since it is a perfect square. If $b \equiv a^2$ then $b^{\phi(n)/2} = a^{\phi(n)} \equiv 1$, so b cannot be a primitive root.

Test $a = 5$*:* Note that $5^2 \equiv 2$, in other words 5 is a square root of 2 (mod 23). This is promising, but we still have to check that $5^{11} \equiv -1$ rather than $+1$. Thus:

$$5^{11} = (5^2)^5 \cdot 5^1 \equiv 2^5 \cdot 5 \equiv 9 \cdot 5 = 45 \equiv -1, \quad yay!$$

So 5 is a primitive root (mod 23).

Having found one primitive root, we don't need to keep testing in order to find all of them. Instead we can use the following observation (essentially the same observation as in Remark 11.13 in the Lecture Notes):

Suppose a is a primitive root mod n. Then $a^i \pmod{n}$ is also a primitive root if and only if GCD$(i, \phi(n)) = 1$.

Hence all the primitive roots (mod 23) are given, mod 23, by

$$5^1, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}.$$

Moreover, since $5^{22} \equiv 1$, the last five of the above are the inverses of the first five (mod 23), in reverse order. For the first five,we just need to compute:

$$5^1 \equiv 5, \quad 5^3 = 5^2 \cdot 5 \equiv 2 \cdot 5 \equiv 10,$$
$$5^5 = 5^3 \cdot 5^2 \equiv 10 \cdot 2 \equiv 20, \quad 5^7 = 5^5 \cdot 5^2 \equiv 20 \cdot 2 \equiv 17,$$
$$5^9 = 5^7 \cdot 5^2 \equiv 17 \cdot 2 \equiv 11.$$

We could keep going, but for the remaining five let's take inverses of these for the fun of it:

$$5^{13} \equiv (5^9)^{-1} \equiv 11^{-1} \equiv -2 \equiv 21,$$
$$5^{15} \equiv (5^7)^{-1} \equiv 17^{-1} \equiv (-6)^{-1} \equiv -4 \equiv 19,$$
$$5^{17} \equiv (5^5)^{-1} \equiv 20^{-1} \equiv (-3)^{-1} \equiv -8 \equiv 15,$$
$$5^{19} \equiv (5^3)^{-1} \equiv 10^{-1} \equiv 7,$$
$$5^{21} \equiv 5^{-1} \equiv 14.$$

So the complete list of primitive roots (mod 23) is: $5,\ 7,\ 10,\ 11,\ 14,\ 15,\ 17,\ 19,\ 20,\ 21$.

3. (i) $132 = 2^2 \cdot 3 \cdot 11$. It's easy to see that 1997 is not divisible by any of 2, 3, 11 (check last digit for 2, digit-sum for 3 and alternating digit-sum for 11) and hence Euler's Theorem applies. $\phi(132) = \phi(2^2) \cdot \phi(3) \cdot \phi(11) = (2^2 - 2^1)(3-1)(11-1) = 2 \cdot 2 \cdot 10 = 40$. Noting that $1997 = 40 \cdot 50 - 3$ and $1997 = 15 \cdot 132 + 17$ we therefore have

$$1997^{1997} \equiv 17^{1997} = (17^{40})^{50} \cdot 17^{-3} \equiv 1^{50} \cdot (17^{-1})^3 \equiv (17^{-1})^3 \pmod{132}.$$

We compute the inverse via Euclid:

$$132 = 7 \cdot 17 + 13,$$
$$17 = 1 \cdot 13 + 4,$$
$$13 = 3 \cdot 4 + 1$$

$$\Rightarrow\ 1 = 13 - 3 \cdot 4$$
$$= 13 - 3(17 - 13)$$
$$= 4 \cdot 13 - 3 \cdot 17$$
$$= 4(132 - 7 \cdot 17) - 3 \cdot 17$$

$$\Rightarrow\ 1 = 4 \cdot 132 - 31 \cdot 17\ \Rightarrow\ 17^{-1} \equiv -31 \pmod{132}.$$

Thus,

$$(17^{-1})^3 \equiv (-31)^3 \equiv -31^2 \cdot 31 \equiv -961 \cdot 31 \equiv -37 \cdot 31 \equiv -1147 \equiv -91 \equiv 41 \pmod{132}.$$

(ii) Clearly, 1994 is divisible by 2, but not by 4 (it is $2000 - 6$) and not by either 3 (check digit-sum) or 11 (check alternating digit-sum). Thus GCD$(1994,\ 132) = 2 > 1$, so we can't use Euler directly. Set $x := 1994^{1994} \pmod{132}$. The trick is to consider x separately modulo a and b, where

- $a \cdot b = 132$,
- a consists of the prime powers in the prime factorisation of 132 which also appear in the prime factorisation of the GCD

- b consists of the remaining prime powers in the factorisation of 132.

Hence, for our example, we take $a = 4$, $b = 33$ and consider $x \pmod 4$ and $x \pmod{33}$.

Mod 4: $1994^{1994} \equiv 2^{1994} \equiv 0$. So $x \equiv 0 \pmod 4$.

Mod 33: This time $\text{GCD}(1994,\, 33) = 1$ so Euler applies. $\phi(33) = (3-1)(11-1) = 20$ and

$$1994^{1994} \equiv 14^{1994} = (14^{20})^{100} \cdot 14^{-6} \equiv 1^{100} \cdot (14^6)^{-1} \equiv ((14^2)^3)^{-1} \equiv ((-2)^3)^{-1} \equiv (-8)^{-1} \equiv 4 \pmod{33}.$$

Summarising, we have

$$x \equiv 0 \pmod 4, \quad x \equiv 4 \pmod{33}.$$

Theorem 11.1 says that there is a unique such x modulo $4 \cdot 33 = 132$. We could use eq. (11.3) to find x, but here it's immediately obvious that $x = 4$ works.

Thus $1994^{1994} \equiv 4 \pmod{132}$.

4. *Step 1:* Since $n = pq$, we first compute $p = n/q = 1961/53 = 37$.
Step 2: Compute $\phi(n) = (p-1)(q-1) = 36 \cdot 52 = 1872$.
Step 3: Compute $d \equiv e^{-1} \pmod{\phi(n)} \equiv 797^{-1} \pmod{1872}$. The numbers are too large for guessing so we apply Euclid. Forwards:

$$\begin{aligned}
1872 &= 2 \cdot 797 + 278, \\
797 &= 2 \cdot 278 + 241, \\
278 &= 1 \cdot 241 + 37, \\
241 &= 6 \cdot 37 + 19, \\
37 &= 1 \cdot 19 + 18, \\
19 &= 1 \cdot 18 + 1.
\end{aligned}$$

Note that this confirms that $\text{GCD}(e,\, \phi(n)) = 1$, which is a requirement for an encryption key. Now backwards:

$$\begin{aligned}
1 &= 19 - 18 \\
&= 19 - (37 - 19) \\
&= 2 \cdot 19 - 37 \\
&= 2(241 - 6 \cdot 37) - 37 \\
&= 2 \cdot 241 - 13 \cdot 37 \\
&= 2 \cdot 241 - 13(278 - 241) \\
&= 15 \cdot 241 - 13 \cdot 278 \\
&= 15(797 - 2 \cdot 278) - 13 \cdot 278 \\
&= 15 \cdot 797 - 43 \cdot 278 \\
&= 15 \cdot 797 - 43(1872 - 2 \cdot 797)
\end{aligned}$$

$$\Rightarrow 1 = 101 \cdot 797 - 43 \cdot 1872,$$

which implies that $d = 101$.

Step 4: The decryption formula is

$$M \equiv M_e^{d_B} \pmod{n_B} \equiv 444^{101} \pmod{1961}.$$

I put this into `Wolfram Alpha` (which, by the way, just runs the repeated squaring algorithm) and got $M = 777$.

5. Since p is a prime, each of the numbers in the set $\{1, 2, \ldots, p-1\}$ has an inverse (mod p) in the same set. The idea is to pair off numbers with their inverses (mod p) in the product $(p-1)!$ such that each pair just gives 1 (mod p). This will prove the result if we can show that the only numbers which are paired off with themselves, i.e.: which are their own inverses (mod p), are 1 and $p-1$, because then the whole product (mod p) will reduce to a bunch of 1:s and $p-1$, which becomes just -1 (mod p). So it remains to prove the following:

Proposition. *Let p be a prime and a an integer not divisible by p. If a is its own inverse (mod p), then $a \equiv \pm 1$ (mod p).*

PROOF: a being its own inverse means that $a \cdot a = a^2 \equiv 1 \pmod{p}$. This means that p divides $a^2 - 1$. But $a^2 - 1 = (a-1)(a+1)$ and, since p is a prime, if p divides a product of two numbers, then it must divide one of them (Key Lemma 7.5 in the Lecture Notes). Thus either

$$p \mid a-1 \ \Rightarrow a \equiv 1 \pmod{p}, \quad \text{or}$$
$$p \mid a+1 \ \Rightarrow a \equiv -1 \pmod{p}, \quad \text{v.s.v.}$$