# Important results (without proof, for now)

1) Define $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. (Euler phi function)

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, for distinct primes $p_1, \dots, p_k$ and for $\alpha_1, \dots, \alpha_k \in \mathbb{N}$, then

$$\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdot (p_2 - 1)p_2^{\alpha_2 - 1} \cdot \dots \cdot (p_k - 1)p_k^{\alpha_k - 1}$$

$$= \prod_{i=1}^{k} (p_i - 1) p_i^{\alpha_i - 1}$$

Notes:

- $\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ product over primes dividing n

- If $m, n \in \mathbb{N}$ are relatively prime ($(m,n)=1$) then $\varphi(mn) = \varphi(m)\varphi(n)$.
  (not true in general if $(m,n) > 1$)

Exs:

1) If $p$ is prime then $|(\mathbb{Z}/p\mathbb{Z})^\times| = \varphi(p) = p - 1$.

2) $n = 9000 = 2^3 \cdot 3^2 \cdot 5^3$

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n) = 9000 \cdot \left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right)\left(1 - \tfrac{1}{5}\right)$$

$$= 9000 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} \cdot \tfrac{4}{5} = 2400$$

2a) Fermat's (little) theorem:

If $p$ is prime, $a \in \mathbb{Z}$, and $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$.

(also stated as: $\forall a \in \mathbb{Z}$, $a^p \equiv a \mod p$)

Ex: Compute $43^{2023} \mod 103$. (find a representative in $\{0, 1, \dots, 102\}$)

Step 1: 103 is prime, and $103 \nmid 43$, so $43^{102} \equiv 1 \mod 103$.

Write $2023 = 19 \cdot 102 + 85$, so that

$$43^{2023} = 43^{19 \cdot 102 + 85} = (\underbrace{43^{102}}_{\equiv 1 \bmod 103})^{19} \cdot 43^{85} \equiv 43^{85} \mod 103.$$

Step 2: Compute $43^{85} \mod 103$.

(Use the Square and multiply algorithm)

- Write 85 in base 2: $85 = 2^6 + 2^4 + 2^2 + 2^0 = 64 + 16 + 4 + 1$
- Successively square 43 until you get to $43^{64} \mod 103$.

$43^1 \equiv 43 \mod 103$

$43^2 = 1849 \equiv 98 \equiv -5 \mod 103$

$43^4 = (43^2)^2 \equiv (-5)^2 \equiv 25 \mod 103$

$43^8 = (43^4)^2 \equiv 25^2 \equiv 7 \mod 103$

$43^{16} = (43^8)^2 \equiv 7^2 \equiv 49 \mod 103$

$43^{32} = (43^{16})^2 \equiv 49^2 \equiv 32 \mod 103$

$43^{64} = (43^{32})^2 \equiv 32^2 \equiv 97 \equiv -6 \mod 103$

• Multiply together the powers that appear in the base 2 expansion of 85:

$$43^{85} = 43^{64+16+4+1} = 43^{64}43^{16}43^{4}43^{1}$$

$$= (-6)\cdot 49\cdot 25\cdot 43 = 57 \mod 103$$

Conclusion: $43^{2023} = 57 \mod 103$.

2b) Euler's theorem:

If $n\in\mathbb{N}$ and $a\in\mathbb{Z}$ satisfies $(a,n)=1$, then $a^{\varphi(n)} = 1 \mod n$.

Notes: • When $n$ is prime, $\varphi(n) = n-1$, so this reduces to Fermat's theorem.

• An even more general result:

If $G$ is a finite group then $\forall g\in G$, $g^{|G|} = e$.

Exs: 1) Find the units digit of $43^{2023}$.

Let $n = 10 = 2^1\cdot 5^1$. Then $(43,n)=1$ and $\varphi(n) = (2-1)(5-1) = 4$, so $43^4 = 1 \mod 10$

$$\Rightarrow 43^{2023} = 43^{4\cdot 505+3} = \underbrace{(43^4)^{505}}_{\text{“}1 \bmod 10\text{”}}\cdot \underbrace{43^3}_{\text{“}3 \bmod 10\text{”}}$$

$$= 3^3 = 7 \mod 10$$

So, the units digit is 7.

2) Find the tens & units digits of "Graham's number":

$$g = 3^{3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}}$$ } more 3's here than you can imagine

Warning:

$$g \neq \left(\left(\left(3^3\right)^3\right)^{3^{\cdots}}\right)^3$$

Idea: We are trying to compute $a^{b_1} \bmod n$,

with $a = 3$, $b_1 = 3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}$, and $n = 100 = 2^2 \cdot 5^2$.

Since $(a,n) = 1$ and $\varphi(n) = 2(2-1)\cdot 5(5-1) = 40$,

we should try to write $b_1 = q_1 \cdot 40 + r_1$,

with $0 \leq r_1 \leq 39$. In other words, we

want to determine $b_1 \bmod 40$.

(next page →)

- Compute $g = 3^{b_1} \bmod 100$, $b_1 = 3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}$ :

$(3,100) = 1$, $100 = 2^2 \cdot 5^2$, $\varphi(100) = 2(2-1)\cdot 5(5-1) = 40$

- Compute $b_1 = 3^{b_2} \bmod 40$, $b_2 = 3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}$ :

$(3,40) = 1$, $40 = 2^3 \cdot 5$, $\varphi(40) = 2^2(2-1)\cdot(5-1) = 16$

- Compute $b_2 = 3^{b_3} \bmod 16$, $b_3 = 3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}$ :

$(3,16) = 1$, $16 = 2^4$, $\varphi(16) = 2^3(2-1) = 8$

- Compute $b_3 = 3^{b_4} \bmod 8$, $b_4 = 3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}$ :

$(3,8) = 1$, $8 = 2^3$, $\varphi(8) = 2^2(2-1) = 4$

- Compute $b_4 = 3^{3^{\cdot^{\cdot^{\cdot^{3}}}}} \bmod 4$:

$$b_4 = (-1)^{\overbrace{3^{\cdot^{\cdot^{\cdot^{3}}}}}^{\text{odd}}} = -1 \bmod 4$$

$$\Rightarrow b_3 = 3^{4q_4 - 1} = (3^4)^{q_4} \cdot 3^{-1} = 3^{-1} = 3 \bmod 8$$

$$\Rightarrow b_2 = 3^{8q_3 + 3} = (3^8)^{q_3} \cdot 3^3 = 11 \bmod 16$$

$$\Rightarrow b_1 = 3^{16q_2 + 11} = (3^{16})^{q_2} \cdot 3^{11} = 27 \bmod 40$$

$$\Rightarrow g = 3^{40q_1 + 27} = (3^{40})^{q_1} \cdot 3^{27} = 3^{27} \bmod 100$$

$$3^{27} = 3^1 \cdot 3^2 \cdot 3^8 \cdot 3^{16} = 3 \cdot 9 \cdot 61 \cdot 21 = 87 \bmod 100.$$

Answer: $g = \cdots\boxed{87}$ .

3) Primitive root theorem: For $n \in \mathbb{N}$, the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 1, 2, 4, p^k$, or $2p^k$, with $p$ an odd prime and $k \in \mathbb{N}$.

If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic then any generator for the group is called a primitive root modulo $n$.

Exs:

1) $n = 7$, $(\mathbb{Z}/7\mathbb{Z})^\times$ is cyclic

$\langle 2 \rangle = \{1, 2, 4\}$

$\langle 3 \rangle = (\mathbb{Z}/7\mathbb{Z})^\times$

primitive root

Scratch work:

| | | |
|---|---|---|
| $2^{3n} = 2^0 = 1$ | $3^0 = 1$ | $3^3 = 6$ |
| $2^{3n+1} = 2^1 = 2$ | $3^1 = 3$ | $3^4 = 4$ |
| $2^{3n+2} = 2^2 = 4$ | $3^2 = 2$ | $3^5 = 5$ |

Note: 5 is also a primitive root, but 1, 4, and 6 are not.

2) $n = 9$, $(\mathbb{Z}/9\mathbb{Z})^\times = \langle 2 \rangle$ (from last time)

primitive roots mod 9 : 2, 5

non-primitive roots mod 9 : 1, 4, 7, 8

3) Given that 5 is a primitive root modulo 103, find all residue classes $x \bmod 103$ which satisfy

$$x^3 \equiv 1 \bmod 103.$$

Write $g=5$. Then (note: $|(\mathbb{Z}/103\mathbb{Z})^\times| = \varphi(103) = 102$)

$(\mathbb{Z}/103\mathbb{Z})^\times = \{\underbrace{g^0}_{=1}, g^1, g^2, \ldots, g^{101}\}$.

Not difficult to show, using the Division Algorithm, that $g^n = 1 \iff n = 102k$ for some $k \in \mathbb{Z}$.

$(n \equiv 0 \bmod 102)$

Every $x \in (\mathbb{Z}/103\mathbb{Z})^\times$ has the form $x = g^m$, for some $0 \le m \le 101$, so we have

$$x^3 = g^{3m} \equiv 1 \bmod 103 \iff 3m \equiv 0 \bmod 102$$

$$\iff m \equiv 0 \bmod \left(\tfrac{102}{3}\right)$$

$$\iff m = 0, 34, \text{ or } 68.$$

Therefore there are three solutions mod 103:

$$x = g^0 = 1 \bmod 103,$$

$$x = g^{34} = 5^{34} = \cdots = 56 \bmod 103, \text{ and}$$

$$x = g^{68} = 5^{68} = \cdots = 46 \bmod 103.$$

4) Chinese remainder theorem: If $n_1, \ldots, n_k \in \mathbb{N}$ satisfy $(n_i, n_j) = 1$, $\forall 1 \le i < j \le k$, (pairwise relatively prime) then $\forall a_1, \ldots, a_k \in \mathbb{Z}$, there is an $x \in \mathbb{Z}$ s.t.

$x \equiv a_1 \bmod n_1$, $x \equiv a_2 \bmod n_2$, $\ldots$, $x \equiv a_k \bmod n_k$,

and this integer $x$ is unique mod $(n_1 n_2 \cdots n_k)$.

Exs: 1) $k=2$, $n_1 = 10$, $n_2 = 21$, $a_1 = 7$, $a_2 = 3$.

Then $(n_1, n_2) = 1$, and we are looking for an integer $x$ satisfying

$$x \equiv 7 \bmod 10 \quad \text{and} \quad x \equiv 3 \bmod 21.$$

Trial and error: $\cancel{3}$, $\cancel{24}$, $\cancel{45}$, $\cancel{66}$, 87

Therefore, the set of all solutions is

$$\{87 + 210m : m \in \mathbb{Z}\}.$$

A "faster" way to find an integer $x$ satisfying the system of equations in the CRT:

- $k=2$: Compute integers $m_1, m_2$ satisfying

$$m_1 \equiv n_1^{-1} \bmod n_2, \quad m_2 \equiv n_2^{-1} \bmod n_1.$$

Then consider $x = n_1 m_1 a_2 + n_2 m_2 a_1$.

mod $n_1$: $x \equiv n_2 m_2 a_1 \equiv a_1 \bmod n_1$,

mod $n_2$: $x \equiv n_1 m_1 a_2 \equiv a_2 \bmod n_2$.

2) $k=2$, $n_1 = 15$, $n_2 = 37$

$a_1 = 8$, $a_2 = 27$

Solve $x = a_1 \bmod n_1$, $x = a_2 \bmod n_2$

Compute:

$m_1 = 15^{-1} \bmod 37$:

| | |
|---|---|
| $37 = 2\cdot 15 + 7$ | $1 = 15 - 2\cdot(37 - 2\cdot 15) = 5\cdot 15 - 2\cdot 37$ |
| $15 = 2\cdot 7 + 1$ | $1 = 15 - 2\cdot 7$ |
| $7 = 7\cdot 1$ | |

$1 = 5\cdot 15 - 2\cdot 37 \Longrightarrow m_1 = 5$ and that $m_2 = -2$

Finally: $x = 15\cdot m_1 \cdot 27 + 37\cdot m_2 \cdot 8 \bmod (15\cdot 37)$

$= 323 \bmod 555$.

Comment: When you already know $m_1 = n_1^{-1} \bmod n_2$, no matter how you found it, there is always a shortcut to compute $m_2 = n_2^{-1} \bmod n_1$:

$$n_1 m_1 = 1 \bmod n_2 \Longrightarrow n_1(-m_1) = -1 \bmod n_2$$

$$\Longrightarrow n_1(-m_1) + 1 = n_2 k,$$

so $k = \dfrac{n_1(-m_1)+1}{n_2} = n_2^{-1} \bmod n_1$.

• $k \geq 3$: First find an integer $x_1$ satisfying

$x_1 \equiv a_1 \bmod n_1$ and $x_1 \equiv a_2 \bmod n_2$.

(Note that $x_1$ is unique mod $n_1 n_2$)

Next, find $x_2 \in \mathbb{Z}$ satisfying

$x_2 \equiv x_1 \bmod n_1 n_2$ and $x_2 \equiv a_3 \bmod n_3$.

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

Finally find $x = x_{k-1}$ satisfying

$x_{k-1} \equiv x_{k-2} \bmod n_1 n_2 \cdots n_{k-1}$ and $x_{k-1} \equiv a_k \bmod n_k$.

3) $k=4$, $n_1=3$, $n_2=5$, $n_3=37$, $n_4=101$,

$a_1=2$, $a_2=3$, $a_3=27$, $a_4=81$

- Solve $x_1 \equiv 2 \bmod 3$, $x_1 \equiv 3 \bmod 5$.

  Brute force (small #'s): $x_1 \equiv 8 \pmod{15}$

- Solve $x_2 \equiv 8 \bmod 15$, $x_2 \equiv 27 \bmod 37$

  $x_2 \equiv 323 \bmod 555$ (example 2)

- Solve $x_3 \equiv 323 \bmod 555$, $x_3 \equiv 81 \bmod 101$

Compute:

$555^{-1} \bmod 101 = 50^{-1} \bmod 101$:

$2 \cdot 50 \equiv -1 \bmod 101 \Rightarrow 50^{-1} \equiv -2 \bmod 101$.

Compute:

$101^{-1} \bmod 555$:

Shortcut: $555 \cdot 2 \equiv -1 \bmod 101 \Rightarrow 555 \cdot 2 + 1 = 101 \cdot k$

Then $k \equiv 101^{-1} \bmod 555$ and $k = 11$.

Finally:

$$x = x_3 = 555\cdot(-2)\cdot 81 + 101\cdot 11\cdot 323 \mod (555\cdot 101)$$

Take $x = 44723$.

Set of all solutions: $\{44723 + 56055\cdot m : m \in \mathbb{Z}\}$

4) Let $n = 605 = 5\cdot 11^2$. Find all residue classes $x \bmod n$ which satisfy the equation

$$x^2 = 1 \mod n.$$

Observation:

$$x^2 = 1 \mod n \overset{\text{(CRT)}}{\iff} x^2 = 1 \mod 5 \quad \text{and} \quad x^2 = 1 \mod (11^2)$$

Plan: Find all $a_1 \bmod 5$ with $a_1^2 = 1 \bmod 5$ and all $a_2 \bmod 121$ with $a_2^2 = 1 \bmod 121$, then combine all pairs of solutions $(a_1 \bmod 5,\ a_2 \bmod 121) \Longrightarrow (x \bmod n)$ using the CRT.

Fact: If $p \geq 3$ is prime and $k \in \mathbb{N}$, then the only solutions to $x^2 = 1 \bmod p^k$ are $x = \pm 1 \bmod p^k$.

Pf: $x^2 = 1 \bmod p^k \iff p^k \mid \underbrace{x^2 - 1}_{=(x-1)(x+1)}$

$\iff p^k \mid x-1$ or $p^k \mid x+1$. $\blacksquare$

(p is prime and $\geq 3$, so it can't divide both $x-1$ and $x+1$)

Using the fact:

$a_1^2 = 1 \bmod 5 \iff a_1 = \pm 1 \bmod 5$, and

$a_2^2 = 1 \bmod 121 \iff a_2 = \pm 1 \bmod 121$.

4 cases: ($n_1 = 5$, $n_2 = 121$, $n = n_1 n_2 = 605$, want $x = a_1 \bmod n_1$, $x = a_2 \bmod n_2$)

- $a_1 = 1$, $a_2 = 1 \Rightarrow x = 1 \bmod n$
- $a_1 = -1$, $a_2 = -1 \Rightarrow x = 604 \bmod n$
- $a_1 = 1$, $a_2 = -1 \Rightarrow x = 241 \bmod n$ (guess and check)

(or... "fast" method):

$n_2^{-1} \bmod n_1 = 1 \bmod n_1$ (take $m_2 = 1$)

$n_2(-m_2) + 1 = n_1 k$

$\Rightarrow k = n_1^{-1} \bmod n_2 = \frac{n_2(-m_2)+1}{n_1} = -24 \bmod n_2$

(take $m_1 = -24$)

$x = n_1 m_1 a_2 + n_2 m_2 a_1 = 241 \bmod 605$

- $a_1 = -1,\ a_2 = 1 \Rightarrow x = 364 \bmod n$ (guess and check)

So, there are 4 solutions mod 605 to $x^2 = 1 \bmod 605$:

$x = 1,\ 241,\ 364,$ and $604 \bmod 605$.