Alin Tomescu, CSE408
Tuesday, March 10th, Lecture #12

More number theory

Theorem from last time (refresher): $\gcd(a,n) = 1 \Leftrightarrow \exists y$, such that $ay \equiv 1\ (mod\ n)$. We write a^{-1} for y.

Theorem: If $\gcd(a,n) = 1$ and $\gcd(b,n) = 1$ then $\gcd(ab,n) = 1$

Proof:

$$\gcd(a,n) = 1 \Leftrightarrow \exists x_1, y_1, ax_1 + ny_1 = 1$$
$$\gcd(b,n) = 1 \Leftrightarrow \exists x_2, y_2, bx_2 + ny_2 = 1$$
$$abx_1x_2 + ax_1y_2n + bx_2y_1n + y_1y_2n^2 = 1$$

$$ab \times x_1x_2 + n \times (something) = 1 \Leftrightarrow \gcd(ab,n) = 1$$

The set of congruence classes modulo n

Notation: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0,1,2, \dots n-1\}$ = congruence class modulo n

Example: $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n | \gcd(x,n) = 1\} = \text{set of all numbers that are coprime to } n$$

$$Z_9^* = \{1,2,4,5,6,7,8\}$$

Properties of $\mathbb{Z}_n^*$

- If you multiply two numbers in $\mathbb{Z}_n^*$ you get another number in $\mathbb{Z}_n^*$ (what the second theorem essentially says)
- $\mathbb{Z}_n^*$ is closed under multiplication. Multiplication is associative in $\mathbb{Z}_n^*$.
- Suppose I pick a number $a \in \mathbb{Z}_n^*$. What is $a \times \mathbb{Z}_n^* = \{a \times x \mid x \in \mathbb{Z}_n^* \}$? It's a subset of $\mathbb{Z}_n^*$. Because $\mathbb{Z}_n^*$ is closed under multiplication.
- $a \in \mathbb{Z}_n^*$ will always have an inverse (according to the first theorem). You can always undo a multiplication.
- Multiplying by $a \in \mathbb{Z}_n^*$ permutes $\mathbb{Z}_n^*$.
    - Take, $a = 5$ you get $a \times \mathbb{Z}_n^* = \{5, 1, 2, 7, 8, 4\}$.

Definition: The totient function, $\varphi(n) = |\mathbb{Z}_n^*|$ is the size of the $\mathbb{Z}_n^*$ set.

Theorem: If $a \in \mathbb{Z}_n^*$, then $a^{\varphi(n)} \equiv 1\ (mod\ n)$.

Proof (by sneakiness):

Since multiplication by a just reoders the numbers, and multiplication is commutative, we have $\prod_{x \in \mathbb{Z}_n^*} x = \prod_{x \in \mathbb{Z}_n^*} ax$.

$$\prod_{x \in \mathbb{Z}_n^*} x = \prod_{x \in \mathbb{Z}_n^*} ax = a^{\varphi(n)} \times \prod_{x \in \mathbb{Z}_n^*} x \Leftrightarrow 1 \equiv a^{\varphi(n)}$$

Side-note: Cancelling works just fine with modular arithmetic when you have an inverse, but that might not always happen. $2x = 2y \bmod 8$ does not imply $x = y$ because you could have $x = 2$ and $y = 6$.

Getting back to our initial problem… How do we go about computing big powers modulo n?

$$5^{77} \bmod 9$$

Alin Tomescu, CSE408
Tuesday, March 10th, Lecture #12

$$\mathbb{Z}_9^* = \{1,2,4,5,7,8\}$$

$$\phi(n) = 6$$

$$77 = 12 \times 6 + 5$$

$$(5^6)^{12} \times 5^5 \; mod \; 9 = 5^5 \; mod \; 9$$

So you can reduce bases mod n and exponents mod $\phi(n)$ in order to perform easy exponentiation. Note that when $n =$ prime then $\phi(n) = n - 1$.

On top of this we can use **logarithmic exponentiation,** after reducing the base and exponents. To give an example of this:

$$a^{128} = ((((((a^2)^2)^2)^2)^2)^2)^2$$

- Instead of performing 128 multiplications, we are only performing $\log_2 128 = 7$.

How to compute the totient function $\phi(n)$?

The totient function has many interesting properties, which can be exploited to easily calculate its values.

$\phi(p) = p - 1$, if n is prime (since all numbers less than p will be coprime with p)

How many numbers between 1 and p^k divide p^k, if p is prime?

- $1, p, 2p, 3p, \ldots, p^k - p$ and p^k all divide p^k
  - A clearer way to express this sequence: $1, 1 \times p, 2 \times p, 3 \times p \ldots (p^{k-1} - 1) \times p, p^{k-1} \times p$
- So there are p^k numbers in total that could "potentially" be coprime to p^k
- p^{k-1} out of these numbers will divide p^k because they will be all the multiples of p from 1 to p^k
  - We exclude the number 1 since even though it divides p^k, it is still considered to be coprime with p^k
  - **Back to 5th grade**: How many multiples of $x > 0$ are there between 1 and n? Answer: $\left\lfloor \frac{n}{x} \right\rfloor$

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

The Chinese remainder theorem

Theorem: If $\gcd(a, b) = 1$ then $\mathbb{Z}_a^* \times \mathbb{Z}_b^* \cong \mathbb{Z}_{ab}^*$

For $\mathbb{Z}_a^* \times \mathbb{Z}_b^* \cong \mathbb{Z}_{ab}^*$ there needs to exist an isomorphism $f : \mathbb{Z}_{ab}^* \to \mathbb{Z}_a^* \times \mathbb{Z}_b^*$ between the two sets, such that:

- f is bijective
- $f(xy) = f(x)f(y), \forall x, y \in \mathbb{Z}_{ab}^*$

But first, how does $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$ "work"?

$$\mathbb{Z}_a^* \times \mathbb{Z}_b^* = \{(x, y) | \; x \in \mathbb{Z}_a^*, y \in \mathbb{Z}_b^*\}$$

- $(x, y) \times (z, w) = (xz \bmod a, yw \bmod b)$, where (x, y) and $(z, w) \in \mathbb{Z}_a^* \times \mathbb{Z}_b^*$
- there exists a neutral element, $(1,1) \times (x, y) = (x, y)$
- there exists an inverse $(x, y) \times (x^{-1}, y^{-1}) = (1,1)$

Proof:

Now, to show that doing arithmetic in $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$ is equivalent to doing arithmetic in $\mathbb{Z}_{ab}^*$ if $\gcd(a, b) = 1$

$$\begin{tikzcd}
x, y \in \mathbb{Z}_{ab}^* \arrow[r, "*"] \arrow[d, "f"'] \arrow[dr, "f(x)f(y) = f(xy)"] & xy \in \mathbb{Z}_{ab}^* \\
x, y \in \mathbb{Z}_a^* \times \mathbb{Z}_b^* \arrow[r, "*"'] & xy \in \mathbb{Z}_a^* \times \mathbb{Z}_b^* \arrow[u, "f^{-1}"']
\end{tikzcd}$$

$Let\ f(x) = (x \bmod a, x \bmod b)$ be our isomorphism. We will prove that it satisfies all the conditions.

1. We need to show that $f(x)$ maps correctly to the codomain. So we need to show that:

$$\gcd(x, ab) = 1 \Rightarrow \gcd(x \bmod a, a) = 1$$

Suppose the above statement is false, then, there exists a common divisor $m > 1$ that divides both $x \bmod a$, and a:

$$m \mid x - ka$$
$$m \mid a$$

Therefore, subtracting the second equality times k from the first equality, we get:

$$m \mid x$$

Then $m \mid ab$ so $\gcd(x, ab)$ would not be 1 anymore. This is a contradiction. Therefore our initial assumption was true.

2. We need to prove that f is invertible.

Since $\gcd(a, b) = 1$, then $\exists r, s$ such that $ra + bs = 1$.

We will define $g\big((x, y)\big) : \mathbb{Z}_a^* \times \mathbb{Z}_b^* \to \mathbb{Z}_{ab}^*$ and prove that $g = f^{-1} \Leftrightarrow f\Big(g\big((x, y)\big)\Big) = (x \bmod a, y \bmod b)$

$$g\big((x, y)\big) = bsx + ray \bmod ab$$

Then $f\Big(g\big((x, y)\big)\Big) = f(bsx + ray \bmod ab) = \big((bsx + ray \bmod ab) \bmod a, (bsx + ray \bmod ab) \bmod b\big)$

Since $a \mid ab$, then $f\big(g(x, y)\big) = (bsx + ray \bmod a, bsx + ray \bmod b) = (bsx \bmod a, ray \bmod b)$

But, $ra + bs = 1 \Leftrightarrow ra = -(bs - 1)$ so $bs \equiv 1\ (mod\ a)$, The other way around, we also get $ra \equiv 1\ (mod\ b)$

$$f\Big(g\big((x, y)\big)\Big) = (x\ mod\ a, y\ mod\ b)$$

3. We need to prove that $\boldsymbol{f(xy) = f(x)f(y), \forall x, y \in \mathbb{Z}_{ab}^*}$

$$f(xy) = (xy\ mod\ a, xy\ mod\ b) = (x\ mod\ a, x\ mod\ b)(y\ mod\ a, y\ mod\ b) = f(x)f(y)$$

Applying the Chinese remainder theorem

Now, we can finally apply the Chinese remainder theorem to compute the totient function:

$$\gcd(a, b) = 1 \Rightarrow \phi(ab) = |Z_{ab}^*| = |Z_a^*||Z_b^*| = \phi(a) \times \phi(b)$$

$$\phi(a) = \phi(a_1^{r_1}) \times \phi(a_2^{r_2}) \times \ldots \times \phi(a_n^{r_n})$$