Lecture 33, Nov. 9

Powers Modulo n

mod 5 in $\mathbb{Z}_5$

x	0	1	2	3	4
x^2	0	1	4	4	1
x^3	0	1	3	2	4
x^4	0	1	1	1	1
x^5	0	1	2	3	4

mod 7 in $\mathbb{Z}_7$

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
x^3	0	1	1	6	1	6	6
x^4	0	1	2	4	4	2	1
x^5	0	1	4	5	2	3	6
x^6	0	1	1	1	1	1	1
x^7	0	1	2	3	4	5	6

mod 20 in $\mathbb{Z}_{20}$

x	0	1	2	3	4	5
x^2	0	1	4	9	16	5
x^3	0	1	8	7	4	.
x^4	0	1	16	1	.	.
x^5	0	1	12	.	.	.
x^6	0	1	4	9	16	5

33.1 Conjecture. for $n \in \mathbb{Z}^+$ 2^{n-1} mod n $\iff$ n is prime. This is false

33.2 Theorem (Fermat's Little Theorem)**.** *let p be a prime then*

1. *for all $a \in \mathbb{Z}$ such that $gcd(a,p) = 1$,*
$$a^{p-1} = 1 \mod p$$

2. *for all $a \in \mathbb{Z}$,*
$$a^p = a \mod p$$

Proof. 1. Let p be prime. Let $a \in \mathbb{Z}$ with $gcd(a,p) = 1$. Then a i invertible in $\mathbb{Z}_p$. Define $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$, by $F(x) = ax$. Note that F is bijective with inverse function $G\colon \mathbb{Z}_p \to \mathbb{Z}_p$, given by $G(x) = a^{-1}x$. Aso note that $F(0) = 0$. So F gives a bijection $F\colon U_p \to U_p$. That is $F\colon \{1,2,3\cdots,p-1\} \to \{1,2,3\cdots,p-1\}$. In other words,
$$\{1,2,3\cdots,p-1\} = \{1\cdot a, 2\cdot a, \cdots, (p-1)\cdot a\}$$
Thus
$$(1\cdot a)(2\cdot a)\cdots((p-1)\cdot a) = 1\cdot 2\cdot 3\cdots(p-1)$$
therefore
$$a^{p-1} = 1$$
in $\mathbb{Z}_p$.

2. Let p be prime. Let $a \in \mathbb{Z}$. If $gcd(a,p) = 1$ in so $p \not| a$ then by 1, we have $a^{p-1} = 1$ in $\mathbb{Z}_p$. So we can multiply both sides by a to get
$$a^p = a$$
in $\mathbb{Z}_p$ If $gcd(a,p) \neq 1$ so $gcd(a,p) = p$ so $p \in a$, then $a = 0 \in \mathbb{Z}$ so $a^p = 0^p = 0 = a \in \mathbb{Z}_p$

$\square$

33.3 Theorem (Euler-Fermat Theorem)**.** *Let $n \in \mathbb{Z}^+$. For all $a \in \mathbb{Z}$ with $gcd(a,n) = 1$,*

$$a^{\varphi(n)} = 1 \mod n$$

Proof. Let $n \in \mathbb{Z}^+$. When $n = 1$ we have $\varphi(n) = 1$. So for $a \in \mathbb{Z}$, $a^{\varphi n} = a^1 = a$.

Suppose $n \geq 2$. Let $a \in \mathbb{Z}$ with $gcd(a,n) = 1$. Since $gcd(a,n) = 1$, we have $a \in U_n$. The function $F\colon U_n \to U_n$ given by $F(x) = ax$ is bijective with inverse $G\colon U_n \to U_n$, given by $G(x) = a^{-1}x$. So the set U_n is equal to the set $\{ax \mid x \in U_n\}$. It follows that
$$\prod_{x \in U_n} (ax) = \prod_{x \in U_n} x$$
then
$$a^{\varphi(n)} = 1$$
in U_n. $\square$

33.4 Theorem. *Let G be a finite commutative group. Then for all $a \in G$,*

$$a^{|G|} = 1$$

(where for a finite set S, $|S|$ denotes the number of elements in S)

Divisibility Test in Base 10

Let $n = \sum_{i=0}^{m} d_i 10^i$ where each $d_i \in \{1, 2, \cdots, 9\}$.

Noto that $2 \mid 10$, so $2^k \mid 10^k$ and $2^k \mid 10^l$ for all $l \geq k$.So

$$10^l = 0 \in \mathbb{Z}_{2^k} \text{ when } l \geq k$$

So in $\mathbb{Z}_{2^k}$,
$$n = \sum_{i=0}^{m} d_i 10^i = \sum_{i=0}^{k-1} d_i 10^i$$

So $2^k \mid n \iff 2^k$ divides the tailing k-digit number of n.

Similarly we have Divisibility Test for $3, 9, 11$.