Number theory: Orders + Exponents

Alexander Remorov

$$3 = 9 \bmod 5$$

$5 \mid 3-8$

$n^2 \bmod 4$ $\quad \begin{matrix} 0 \\ 1 \end{matrix}$

~~2~~

~~3~~

$a = c \bmod n \qquad b = d \bmod n$

$$a+b = c+d \bmod n$$
$$a-b = c-d \bmod n$$
$$ab = cd \bmod n$$

$a = c \bmod n \qquad a = c + kn.$

If $\gcd(a, n) = 1$ you can find f so $af = 1 \bmod n$.

$$\underbrace{a \times a \times a \ldots \times a}_{m \text{ times}} = \underbrace{c \times c \times c \ldots \times c}_{m \text{ times}} \bmod n$$

$$a^m = c^m \bmod n.$$

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + xy^{n-2} + y^{n-1})$$

$$x^2 - y^2 = (x-y)(x+y)$$

Fill in $y = -y$

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \dots)$$

Binomial Theorem:

$$(a+b)^n = a^n + n a^{n-1}b^1 + \frac{n(n-1)}{2!}a^{n-2}b^2 + \dots + b^n$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

When we work mod p where p is a prime.

$$(a+b)^p \bmod p$$

$$= a^p + p a^{p-1} b + \frac{p(p-1)}{2!} a^{p-2} b^2 + \cdots + \frac{p(p-1)(p-2)\cdots 2}{(p-1)(p-2)\cdots 1} a^1 b^{p-1} + b^p \bmod p$$

$$= a^p + 0 + 0 + \cdots + 0 + b^p \bmod p$$

$$= a^p + b^p \bmod p.$$

$$\underline{(a+b)^p} = \underline{a^p + b^p \bmod p.}$$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \leftarrow \text{divisible by } p \text{ if } k \neq 0 \text{ or } p.$$

Fermat's Little Theorem: If p is prime then $a^p = a \bmod p$.

Pf Note if $a=0$ $a^p = 0^p = 0$.

so $a^p = 0 = a \bmod p$.

This works when $a=0$.

Assume true for k and prove for $k+1$.

⊛ $k^p = k \bmod p$.

$(k+1)^p = k^p + 1^p = k+1 \bmod p$. ▩

$$2^{130} \bmod 13$$

$$= \underbrace{2^{13} \times 2^{13} \times 2^{13} \cdots \times 2^{13}}_{10} \bmod 13$$

$$= 2 \times 2 \times 2 \times \cdots \times 2 \bmod 13$$

$$= 2^{10} \bmod 13$$

$$= 1024 \bmod 13.$$ ▩

If $\gcd(a,p)=1$ then

$a^{p-1} = 1 \bmod p$.

→ $a^p = a \bmod p$ and we know of $\gcd(a,p)=1$ we can find f so

$af = 1 \bmod p$

$fa^p = fa \bmod p$

$fa\ a^{p-1} = 1 \bmod p$.

E.g. What is the last digit of 7^{2021}?

$7^{2021} \bmod 10$. ① $7^{2021} \bmod 2$ ② $7^{2021} \bmod 5$.

① $7^{2021} \bmod 2 = 1^{2021} \bmod 2 = 1 \bmod 2$.

② $7^{2021} \bmod 5 = 2^{2021} \bmod 5$

$= 2^{2020} \times 2^1 \bmod 5$

$= (2^{305})^4 \times 2 \bmod 5$

$= 1 \times 2 \bmod 5$

$= 2 \bmod 5$.

My answer is $1 \bmod 2$ and $2 \bmod 5$.

3, (7)

So the last digit is 7.

If we have a whole number n

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

$$120 = 2 \times 60 = 2^2 \times 30 = 2^3 \times 15 = 2^3 \times 3^1 \times 5^1$$

$$120 = 2^3\ 3^1\ 5^1 = p_1^{e_1} p_2^{e_2} p_3^{e_3}$$

$p_1 = 2 \quad e_1 = 3$

$p_2 = 3 \quad e_2 = 1$

$p_3 = 5 \quad e_3 = 1.$

mod 2, mod 5 $\Rightarrow$ mod 10

How many factors does 12 have?

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

✓ ✓ ✓ ✓ ✓ ✓

How many factors does

$\rightarrow n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ have?

If m is a factor

$$m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

$0 \le f_1 \le e_1, \quad 0 \le f_2 \le e_2 \quad \cdots \quad 0 \le f_k \le e_k$

$(e_1+1) \quad (e_2+1) \quad \cdots \quad (e_k+1)$

$12 = 2^2 \times 3^1$

$(2+1)(1+1) = 3 \times 2 = 6.$

$120 = 2^3 \times 3^1 \times 5^1$

$(3+1)(1+1)(1+1) = 4 \times 2 \times 2 = 16.$

If $\gcd(a,p)=1$

$$a^{p-1} \equiv 1 \mod p.$$

The idea of finding a number d so that

$$a^d \equiv 1 \mod n$$

can be really useful. The smallest positive number e so that

$$a^e \equiv 1 \mod n$$

is called the order of a mod n, $\operatorname{ord}_n a = e$.

You can show that if

$$a^d \equiv 1 \mod n$$

then d is divisible by $e = \operatorname{ord}_n a$.

Pf Divide d by e and get a remainder r. $d = ke + r$

and $0 \le r < e$.

$$a^d = a^{ke+r} = a^{ek} a^r = \underbrace{a^e a^e a^e \cdots a^e}_{k} a^r \mod n$$

$$\to 1 = 1 \cdot 1 \cdot 1 \cdots 1 \cdot a^r \mod n$$

i.e. $a^r \equiv 1 \mod n$, $\Rightarrow r = 0$.

So $d = ke$, so e divides into d. ∎

Ex. Look at $2^m \mod 7$.

m	$2^m \bmod 7$	
0	1	
1	2	
2	4	
→ 3	1	← $\operatorname{ord}_7 2 = 3$.
4	2	
5	4	
→ 6	(1)	← also $2^6 \equiv 1 \mod 7$

Euler's Theorem is like Fermat's Little Theorem, but works for numbers that are not prime.

12: $\gcd(a,12) = 1$.

1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	1	6	1	4	3	2	1	12.

Number of invertible numbers is 4.

$\phi(n)$ is the # of invertible numbers mod n.

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$$= p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$$\longrightarrow = p_1^{e_1-1} p_2^{e_2-1} \cdots p_k^{e_k-1}(p_1-1)(p_2-1)\cdots(p_k-1).$$

Euler's Theorem If $\gcd(a,n) = 1$

then $a^{\phi(n)} = 1 \mod n$.

E.g. If n is prime, $n = p$

$\phi(n) = p-1$, $a^{\phi(p)} = a^{p-1} = 1 \mod n$.

Q2 Let p be prime and $P(x)$ is a polynomial with integer coefficients. $P(0), P(1) \ldots P(p^2-1)$ are all different mod p^2, prove $P(0), P(1), \ldots P(p^3-1)$ are all different mod p^3.

Q3 (IMO 1991) Let n be an integer > 6. Let $a_1, a_2, \ldots a_k$ be positive integers relatively prime to n and

$$a_2 - a_1 = a_3 - a_2 = \cdots = a_k - a_{k-1} > 0$$

Show that n is a prime or n is a power of 2.

David.Malone@mu.ie.