Chapter 6
Some Special Congruences

邱錫彥 老師

Contents

6.1 Wilson's theorem

- Thm: If p is prime, then $(p-1)! = -1 \bmod p$
- Proof: When $p = 2$, $(p-1)! = 1! = 1 = -1 \bmod 2$.

  When $p = 3$, $(p-1)! = 2! = 2 = -1 \bmod 3$.

  When $p \geq 5$, $\forall\, a$, $1 \leq a \leq p-1$, $\exists\, a^{-1}$, $1 \leq a^{-1} \leq p-1$

  $\rightarrow aa^{-1} = 1 \bmod p$

  the only positive integers less than p
  that are their own inverse are 1 and p-1.

  We have $\prod_{i=2}^{p-2} i = 1 \bmod p$

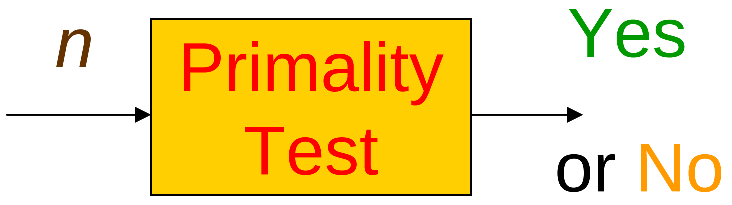
  $$(p-1)! = \prod_{i=1}^{p-1} i = 1 \times \prod_{i=2}^{p-2} i \times (p-1) = p-1 = -1 \bmod p$$

- Thm: If $n \in Z^+$ and $(n-1)! = -1 \bmod n$, then n is prime.
- Proof: Let $n = ab$, $1<a<n$, $1<b<n$, and $(n-1)!=-1 \bmod n$

  $a|n$ and $a|(n-1)!$, $n|(n-1)!+1$

  $a|[(n-1)!+1-(n-1)!]=1$,

  This is a contradiction since $a>1$



e.g. $(n\text{-}1)! = -1 \bmod n$ iff n is prime

- Deterministic:
  If the output is Yes, then *n* is prime certainly.
- Probabilistic:
  If the output is No, then *n* is composite.
  If output is Yes, then the probability that *n* is prime is $1-\varepsilon$, where ε, less than 1, can be controlled.

- Primality test by using Wilson's theorem.
- Input: n
- Output: Yes or No
- Algorithm: compute $(n-1)!=a \bmod n$

  if $a=-1$, then output "Yes"

  otherwise, output "No"
- Complexity: $(n-2)$ multiplications

  $\Rightarrow O(n(\log_2 n)^2)$ bit operation

Fermat's little theorem

- Thm: If p is prime and $a \in Z^+$ with $p \nmid a$, then $a^{p-1}=1 \bmod p$.

Proof:

Since $p \nmid a$, $\Rightarrow p \nmid ja$, $1 \leq j \leq p\text{-}1$,

But $\{1,2,\ldots,p\text{-}1\}=\{a,2a,\ldots(p\text{-}1)a\}$

$$\Rightarrow \prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} ia$$

$$\Rightarrow (p-1)! = a^{p-1}\prod_{i=1}^{p-1} i = a^{p-1}(p-1)! = \bmod p$$

$\because ((p\text{-}1)!, p) = 1$

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

- Thm: If p is prime and $a \in Z^+$, then $a^p - a = 0 \bmod p$
- Proof: If $p|a$, then $p|a^p \Rightarrow a^p - a = 0 \bmod p$

  If $p \nmid a$, then $p|a^{p-1} - 1 \bmod p \Rightarrow a^p - a = 0 \bmod p$
- Thm: If p is prime and $a \in Z^+$, with $p \nmid a$, then

  $a^{-1} = a^{p-2} \bmod p$
- Proof: If $p \nmid a$, then $a^{p-1} = 1 \bmod p \Rightarrow a \cdot a^{p-2} = 1 \bmod p$

  $\Rightarrow a^{-1} = a^{p-2} \bmod p$
- Corollary: If $a, b \in Z^+$ and p is prime with $p \nmid a$, then the solution of $ax = b \bmod p$ is

  $x = a^{p-2} b \bmod p$

- Pollard P-1 method:

  Factor n, when n has a prime factor $p \rightarrow$ the prime dividing p-1 are relatively small.

  Assume $p|n$, and $(p-1)|k!$, where k is a predetermined positive integer.

  Input:n

  output:p

Algorithm 1:

1.Find $M=2^{k!}-1 \bmod n$, where $M \neq 0$

since $2^{k!}=1 \bmod p$(if $(p-1)|k!$)

$p|M=2^{k!}-1 \bmod n$

2.Compute $(M,n)=d$, then d is an ontrivial divisor of n.

Algorithm 2:

Let $p-1=\prod p_i^{a_i}$, $p_i<R$ and $a_i \leq \max\{a_i\}=A$

1.Find $\prod q_i^A$(q_i is prime)$\Rightarrow p-1|R$

2.Compute $M=2^R-1 \bmod n$, where $M=0$

3.Compute $(M,n)=d$, then d is a nontrivial divisor of n.

- Problem :How to compute a k! mod n efficiently?
- Algorithm:Let $r_1=a$,

  For i=2 to k,

  $r_i=r_{i-1}^{\ i}$ mod n

  output r_k

- $a^{5!}=((((a^1)^2)^3)^4)^5$ mod n
- Remark:In general, B cannot be too large,otherwise

  Pollard P-1 method cannot work properly.

  (B<1000)

6.2 PseudoPrime

- Ancient Chinese conjectured that if $2^n = 2 \bmod n$, then n must be prime.
- Fact: If n is prime, then $b^n = b \bmod n$, $\forall b \in Z^+$
- Problem: If $b^n = b \bmod n$, is n prime? Ans: No.
- Ex: $n = 341 = 11 \times 31$

  $2^{10} = 1 \bmod 11 \Rightarrow 2^{340} = 1 \bmod 11$

  $2^5 = 1 \bmod 31 \Rightarrow (2^5)^{68} = 2^{340} = 1 \bmod 31$

  $2^{340} = 1 \bmod 341$

  $2^{341} = 2 \bmod 341$

  but 341 is composite

- Def: Let $b \in Z^+$. If n is a composite positive integer
  and $b^n = b \bmod n$, then
  n is called a pseudoprime to the base b.
- Remark:If $(b,n)=1$, then $b^n=b \bmod n$ is equivalent to
  $b^{n-1}=1 \bmod n$.
- Ex: $341=11\times 31$, $561=3\times 11\times 17$ and $645=3\times 5\times 43$ are
  pseudoprimes to the base 2.
- Problem:Given $b\in Z^+$,how many pseudoprimes to
  the base b?
- Ans: Infinitely many pseudoprimes to any given base
- Prove the answer for the base 2.

- Lemma: If $d, n \in Z^+$ and $d|n$, then $2^d-1|2^n-1$

  Proof: $d|n$, $\exists t \rightarrow dt=n$

  $2^{dt}-1=(2^d-1)(2^{d(t-1)}+2^{d(t-2)}+\ldots+1)$

  $\Rightarrow (2^d-1)|(2^n-1)$

- Thm: There are infinitely many pseudoprimes to the base 2.

- Proof:1.If n is an odd pseudoprime to the base 2, then $m=2^n-1$ is also an odd pseudoprime to the base 2, because $n=341$ is a pseudoprime to the base 2, we can conclude that there are infinitely many pseudoprimes to the base 2.

2. Let $n=dt$ be an odd pseudoprime,

n is composite and $2^{n-1}=1 \bmod n$,

Let $m=2^n-1$, then

(a) m is composite since $2^d-1|(2^n-1)=m$

(b) since $2^n=2 \bmod n$, so $\exists k \in Z$ $2^n-2=kn$

$\Rightarrow 2^{m-1}=2^{2^n-2}=2^{kn} \Rightarrow m=(2^n-1)|(2^{kn}-1)=2^{m-1}-1$

$\Rightarrow 2^{m-1}-1=0 \bmod m, 2^{m-1}=1 \bmod m$

We have that m is also a pseudoprime to the base 2

- If n is a pseudoprime to the base b, it does not imply that n is also a pseudoprime to the base b', where $b' \neq b$.

- Ex: 341 is a pseudoprime to the base 2, but not to the base 7.
- A Primality Test Method is as follow:

Input: n

(1) Choose $1<b<n$, and compute

$$b^{n-1} = a \bmod n,$$

if $a \neq 1$,

then output "n is composite".

(2) repeat (1) k times.

(3) output "n may be prime".

- Remark:

1. If the output of the method is "n is composite", the n must be composite
2. If k is increased, then the probability that "n is composite" is decreased.

- Question: If $k \rightarrow \infty$, does the probability = 0?

  Or $\exists$ composite integers $n \rightarrow b^{n-1}=1 \bmod n$, b with $(b, n) = 1$?

- Def:A composite integer that satisfies $b^{n-1}=1 \bmod n$, $b \in Z^+$ and $(b,n)=1$, is called a Carmichael number

Ex: Prove that $561 = 3 \times 11 \times 17$ is a Carmichael number.

Proof:

Let $b \in Z^+$ with $(b,561)=1$. Then $(b,3)=(b,11)=(b,17)=1$

$\Rightarrow b^2 = 1 \bmod 3$, $b^{10} = 1 \bmod 11$, $b^{16} = 1 \bmod 17$,

$\because 2|560, 10|560$, and $16|560$,

$\Rightarrow b^{560}=1 \bmod 3$, $b^{560}=1 \bmod 11$, $b^{560}=1 \bmod 17$

$\Rightarrow b^{560}=1 \bmod 561$, $\forall b$ with $(b,n)=1$.

- It is conjectured that there are infinitely many Carmichael numbers, but so far this has not been demonstrated.

Conditions for producing Carmichael number

- Thm: If $n = q_1 q_2 \ldots q_k$, where q_i is prime
  and $q_i \neq q_j$, $\forall\ 1 \leq i, j \leq k$,
  and $(q_j-1)|(n-1)$, $\forall\ j$.
  Then n is a Carmichael number.
- Proof:Let $b \in Z^+$ and $(b, n)=1$, then $(b, q_j)=1$, $1 \leq j \leq k$

$$b^{q_j-1} = 1 \bmod q_j, 1 \leq j \leq k$$

$$(q_j-1)|(n-1) \Rightarrow b^{n-1} = 1 \bmod q_j, 1 \leq j \leq k$$

By CRT, we see that $b^{n-1} = 1 \bmod n$

$\Rightarrow n$ is a Carmichael number.

- Remark:

All Carmichael numbers must be of the form

$$n = q_1 q_2 \ldots q_k$$

where the q_j's are distinct primes and

$$(q_j - 1) | (n - 1),$$

$1 \leq j \leq k.$

[*Proof* is shown in chapter 8]

- Let n be an odd integer.

  If $b^{n-1}=1 \bmod n$, then n is either a prime or a pseudoprime to the base b.

  If n is a prime, then $b^{(n-1)/2} = \pm 1 \bmod n$

  If n is a pseudoprime to the base, then it's possible that $b^{(n-1)/2} \neq \pm 1 \bmod n$

n, odd →

Randomly choose b, $1 \leq b \leq n-1$
If $b^{(n-1)/2} \neq \pm 1 \bmod n$
then n is composite

- Def: Let $n \in Z^+$ and n-1=$2^s t$, where s, $t \in Z^+$ and t is odd. We say that n passes **Miller's test** for the base b, if either $b^t = 1 \pmod{n}$ or $b^{2^j t} = -1 \bmod n$ for some j with $0 \le j \le s-1$.
- Thm: If n is prime and b is a positive integer with $n \nmid b$, then n passes Miller's test for the base b.

Proof: Let $n-1=2^s t$, where $s,t \in Z^+$ and t is an odd integer

Let $x_k = b^{(n-1)/2^k} = b^{2^{s-k} t}$, for k=0,1,2,…,s

$\because n$ is prime, $x_0 = b^{n-1} = 1 \bmod n$.

$x_1^2 = x_0 = 1 \bmod n \Rightarrow x_1 = 1 \bmod n$ or $x_1 = -1 \bmod n$

If $x_1=-1 \bmod n \Rightarrow n$ passes Miller's test for the base b.

If $x_1=1 \bmod n$ then $x_2^2=x_1=1 \bmod n \Rightarrow x_2=1$ or $x_1=-1 \bmod n$.

In general, if $x_0=x_1=\ldots=x_k=1 \bmod n$, with $k<s$, we know that either $x_{k+1}=-1 \bmod n$ or $x_{k+1}=1 \bmod n$.

Continuing this procedure for $k=0,1,2,\ldots,s$, we find that either $x_k=1 \bmod n$ for $k=0,1,2,\ldots,s$, or $x_k=-1 \bmod n$ for some integer k. n passes Miller's test for the base b.

- Def: If n is composite and passes Miller's test for the base b, then we say n is a strong pseudoprime to the base b.
- Thm: There are infinitely many strong pseudoprimes to the base 2.

Proof Strategy:

If n is a pseudoprime to the base 2, then

2^n-1 is an pseudoprime and a strong pseudoprime

to the base 2.

- Proof: If n is composite and $2^{n-1}=1 \bmod n, 2^{n-1}-1=nk$, $k \in Z^+$ and k is odd. $N-1=(2^n-1)-1=2^n-2=2nk$.

Note that $2^{(N-1)/2}=2^{nk}=(2^n)^k=1 \bmod N$

$(\because 2^n=(2^n-1)+1=N+1)$

there are infinitely many strong pseudoprimes to the base 2.

- Thm: If n is an odd composite positive integer, then n passes Miller's test for at most $(n-1)/4$ bases b, with $1 \le b \le n-1$. (will be proven in chapter 8)

- Thm: **Rabin's probabilistic primality test**.

  Let $n \in Z^+$ and n is odd.
  Pick k different positive integers less than n and perform Miller's test on n for each of these bases.
  If n is composite, the probability that n passes all k tests is less than $(1/4)^k$.

- Complexity: $O((\log_2 n)^4)$

- *Generalized Riemann hypothesis* (a famous conjecture): Deterministic primality test

- Conjecture: For every composite positive integer n, there is a base b with $b < 2(\log_2 n)^2$ such that n fails Miller's test for b.

- Thm: If the *generalized Riemann hypothesis* is valid. Then there is an algorithm to determine whether a positive integer n is prime using $O((\log_2 n)^5)$ bit operations.
- Proof: Miller's test needs $O((\log_2 n)^3)$ bit operations
  $1<b<2(\log_2 n)^2$, we need $O((\log_2 n)^2)$ Miller's tests.
  We need $O((\log_2 n)^5)$ bit operations to determine whether n is composite or prime.

- Important facts:

  To factor n needs subexponential time.

  To determine n is prime needs polynomial time.

6.3 Euler's Theorem

- Def: Let $n \in Z^+$,the Euler phi-function $\phi(n)$ is defined to be the number of positive integers not exceeding n that are relatively prime to n.
- Ex: $\phi(10) = 4$.
  1,3,7,9 (less than 10) are relatively prime to 10.

Note: Compared with $\pi(x)$,
defined in "3.1 Prime numbers."

- Def: A reduce residue system modulo n is a set of $\phi(n)$ integers, such that each element of the set is relatively prime to n, and no two different elements of the set are congruent modulo n.

- $s = \{a_1, a_2, \ldots, a_{\phi(n)}\}$, where $(a_i, n) = 1$, $1 \le i \le \phi(n)$ and $a_i \neq a_j \bmod n$
- Note: $|s| = \phi(n)$

- Thm: Let $s = \{r_1, r_2, \ldots, r_{\phi(n)}\}$
  be a reduced residue system modulo n.
  If $(a,n)=1$, $a \in Z^+$, then the set
  $s' = \{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$
  is also a reduced residue system modulo n.

- Proof: $(a, n) = 1$ and $(r_j, n) = 1$
  $\Rightarrow (ar_j, n) = 1$, $j = 1,2,\ldots,\phi(n)$
  $\Rightarrow ar_j \neq ar_i \bmod n$, $j \neq i$.
  So s' is a reduced residue system modulo n.

Euler's Theorem

- Thm: If $m \in Z^+$ and $a \in Z$ with $(a, m) = 1$, then
  $a^{\phi(m)} = 1 \bmod m$.
- Proof:
  Let $s = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ and $s' = \{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ be two reduced residue system modulo m, where $(a,m) = 1$, then

$$\prod_{j=1}^{\phi(m)} r_j = \prod_{j=1}^{\phi(m)} ar_j = a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \bmod m$$

$$\left(\prod_{j=1}^{\phi(m)} r_j, m\right) = 1 \Rightarrow a^{\phi(m)} = 1 \bmod m$$

- Remark:

1. If m is prime, then Euler's Theorem is equivalent to Fermat's Little Theorem.
2. If $(a, m) = 1$,then $a^{-1} = a^{\phi(n)-1} \mod m$
3. If $(a, m) = 1$, the solution of $ax = b \mod m$ is

$$x = a^{\phi(m)-1}b \mod m$$

- Problem: Given m, how can we find $\phi(m)$?