LMAT2440 – Théorie des Nombres

Olivier Pereira – Jean-Pierre Tignol

2014–2015

Algorithmic Number Theory

Study of Numbers

vs.

Study of **this** Number

Algorithmic Number Theory

There are infinitely many primes.

vs.

1267650600228229401496703205653 is prime.

Algorithmic Number Theory

Every integer greater than 1 is either prime itself or is the product of prime numbers.

vs.

$$2535301200456606295881202795651 = 1125899906842679 \times 2251799813685269$$

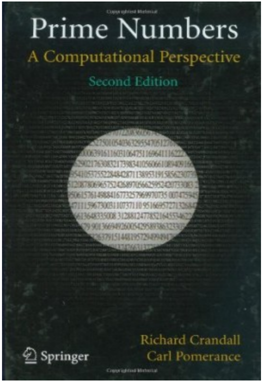
Plan

1. Primality testing/proving
2. Integer factorization
3. Engineering elliptic curves for cryptographic use
4. Engineering encryption from residuosity class problems

Schedule

- Lectures on 21/11, 28/11, 03/12, 10/12
- Exercises on 05/12 and 12/12

Reference



- *Prime Numbers. A computational Perspective.* By R. Crandall and C. Pomerance, Springer, 2nd Edition.

Recognizing Primes
Strategy 1 : Trial Division

prime $\leftarrow$ *True*
$d \leftarrow 2$
while $d \leq \sqrt{n}$ **do**
  if $d|n$ **then**
    prime $\leftarrow$ *False*
    break
  $d \leftarrow d + 1$
return *prime*

Complexity $\approx p$ divisions, with p smallest factor

Improvements :

- Clear 2, then $d \leftarrow d + 2$
- Clear 2, 3, then $+2, +4, +2, +4, +2, \ldots$
- Sequence has length 30 when clearing 2, 3, 5, 7
- Sequence has length 1.021.870.080 when clearing primes < 30, and saves 52% work compared to clearing 2, 3
- Trying only primes $\leq \sqrt{n}$ $\Rightarrow \approx \frac{\sqrt(n)}{\ln(n)/2}$ divisions

Sieve of Eratosthenes (276–194)

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Sieve of Eratosthenes (276–194)

$prime\_list \leftarrow [True]^n$
for $d \leftarrow [2, \sqrt{n}]$ **do**
  if $prime\_list[d]$ **then**
    for $i \leftarrow \{d^2, d^2 + d, \ldots, \leq n\}$ **do**
      $prime\_list[i] \leftarrow False$
return $prime\_list$

Complexity (if only additions) :
$\sum_{p \in P_{\sqrt{n}}} n/p - p \leq \sum_{p \in P_{\sqrt{n}}} n/p \approx n \ln \ln n$

Only $\ln \ln n$ operations/integer !

Fermat pseudoprimes

$$a^n \equiv a \pmod{n}$$

- Always true if n is prime
- A composite n is a *pseudoprime base a* if (n, a) satisfy this equation

Recognizing Primes
Strategy 2 : Fermat's test

for $i \leftarrow [1, t]$ **do** ▷ Repeat t times

  $a \xleftarrow{r} [2, n-1]$ ▷ Select random basis

  if $a^n \not\equiv a \pmod{n}$ **then** ▷ Test Fermat's equality

    return *composite* ▷ If fails, then composite

return *probable prime* ▷ Else, probable prime

Fermat pseudoprimes

1. For each a, there are infinitely many pseudoprimes base a

   If p is an odd prime not dividing $a^2 - 1$ then
   $n = (a^{2p} - 1)/(a^2 - 1)$ is pseudoprime base a

Fermat pseudoprimes

2. **Carmichael numbers :** A composite n is a *Carmichael number* if $a^n = a \pmod{n}$ for every integer a

   If n is composite, squarefree and $\forall p|n : p-1|n-1$, then n is a Carmichael number.
   Ex : 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, ...

   Proof :

   - If n si squarefree $\Rightarrow$ just show $a^n = a \pmod{p}$, $\forall p|n$
   - Let $p|n$ and $a \in \mathbb{N}$
   - If $p|a$ then $p|a^n - a$
   - if $p \not| a$ then $a^{p-1} = 1 \bmod p$ and $a^{n-1} = 1 \pmod{p}$ since $p-1|n-1$.

Fermat pseudoprimes

3. If n is composite and not pseudoprime base $a \in \mathbb{Z}_n^*$ then it is not pseudoprime for at least $\varphi(n)/2$ bases.

Proof :

- If n is pseudoprime base $b \in \mathbb{Z}_n^*$, then it is not pseudoprime base ab : $(ab)^n = a^n b^n = a^n \neq a \bmod n$
- If $b_1, b_2 \in (\mathbb{Z}_n^*)^2$ then $ab_1 \neq ab_2$

Euler(-Jacobi) pseudoprimes

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

- Always true if n is prime and $n \not| a$
- A composite n is a *Euler pseudoprime base a* if (n, a) satisfy this equation

Recognizing Primes
Strategy 3 : Solovay-Strassen's test

for $i \leftarrow [1, t]$ **do** $\triangleright$ Repeat t times

  $a \xleftarrow{r} [2, n-1]$ $\triangleright$ Select random basis

  if $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$ **then** $\triangleright$ Test Euler's criterion

    return *composite* $\triangleright$ If fails, then composite

return *probable prime* $\triangleright$ Else, probable prime

Euler(-Jacobi) pseudoprimes

1. If n is composite and not pseudoprime base $a \in \mathbb{Z}_n^*$ then it is not pseudoprime for at least $\varphi(n)/2$ bases.

   Proof : Same multiplicativity property with Jacobi's symbol

Euler(-Jacobi) pseudoprimes

2. If n is composite, then there is always a base a such that n is *not* pseudoprime base a.

Proof : *Part 1 :* if $p^2|n$ then $a = 1 + \frac{n}{p}$ is a witness

- $(1 + \frac{n}{p})^p = 1 + n + B(p, 2)pn + \cdots \equiv 1 \bmod n$
- Then $(1 + \frac{n}{p})^j \equiv 1 \bmod n$ implies $p|j$.
  Otherwise, $\gcd(p, j) = 1$ and $\forall x, \exists a, b$ such that $x = aj + bp$ and $(1 + \frac{n}{p})^x = 1 \bmod n$.
- If a is not a witness, then $a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$ and $a^{n-1} \equiv 1 \bmod n$. But $p \not| n - 1$, so a must be a witness.

Euler(-Jacobi) pseudoprimes

2. If n is composite, then there is always a base a such that n is *not* pseudoprime base a.

Proof : *Part 2 :* if n is squarefree and $p|n$

- Suppose $\exists a : a = 1 \bmod \frac{n}{p}$ and $\left(\frac{a}{p}\right) = -1$.
- Then $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{\frac{n}{p}}\right) = -1\left(\frac{1}{a}\right) = -1$
- Then $a^{\frac{n-1}{2}} = 1 \bmod \frac{n}{p}$ and $a^{\frac{n-1}{2}} = 1 + j\frac{n}{p} \bmod n$. But $1 + j\frac{n}{p} \neq -1 \bmod n$ since $-2 \not| \frac{n}{p}$.
- So, a would be a witness. But does it exist ?
- Pick $b : \left(\frac{b}{p}\right) = -1$. Then the system $a = b \bmod p$ and $a = 1 \bmod \frac{n}{p}$ has a solution (since $\gcd(p, \frac{n}{p}) = 1$) !

Strong pseudoprimes

Let $n - 1 = 2^s t$ where t is odd

$$a^t \equiv 1 \pmod{n}$$
$$\text{or}$$
$$a^{2^i t} \equiv -1 \pmod{n} \text{ for some } i \in [0, s[$$

- Always true if n is prime and $n \not| a$
- A composite n is a *strong pseudoprime base a* if (n, a) satisfy this equation

Recognizing Primes
Strategy 4 : Miller-Rabin test

Let $n - 1 = 2^s t$

```
for i ← [1, u] do                                  ▷ Repeat u times
    a ←r [2, n − 1]                                ▷ Select random basis
    b ← a^t mod n                                  ▷ Computing "smallest" root
    if b ≡ ±1 (mod n) then
        break                                      ▷ n looks prime
    for r ← [0, s[ do                              ▷ Checking squares
        b ← b^2
        if b = 1 then
            return composite                       ▷ Got 1 before -1
        if b = −1 then
            break                                  ▷ n looks prime
    return composite                               ▷ Never got 1
return probable prime                              ▷ We tried enough
```

Strong pseudoprimes

1. For each composite $n > 9$:
   $|\{\text{strong pseudoprimes bases mod } n\}| \leq \frac{1}{4}\varphi(n) \leq \frac{n}{4}$

   Proof :(for the case where $p^2|n$ only)

   Ex cursus : $\mathbb{Z}^*_{p^2}$ is cyclic of order $p(p-1)$
   - Let g be a generator of $\mathbb{Z}^*_p$
   - If $g^{p-1} \neq 1 \bmod p^2$ then g is of order $p(p-1)$
     Indeed, order of g divides $p(p-1)$ and
     $g^p \equiv g \pmod{p} \Rightarrow g^p \equiv g + ip \not\equiv 1 \pmod{p^2}$
   - If $g^{p-1} = 1 \bmod p^2$ then $g(1+p)$ is of order $p(p-1)$
     Indeed, $(g(1+p))^{p-1} = (1+p)^{p-1} = 1 + (p-1)p = 1 - p \neq 1 \bmod p^2$

Strong pseudoprimes

1. For each composite $n > 9$:
   $|\{\text{strong pseudoprimes bases mod } n\}| \leq \frac{1}{4}\varphi(n) \leq \frac{n}{4}$

   Proof :(for the case where $p^2|n$ only)

   - If $a^{n-1} \equiv 1 \bmod n$ then $a^{n-1} \equiv 1 \bmod p^2$
   - If g generates $\mathbb{Z}^*_{p^2}$ then $\exists j : a = g^j \bmod p^2$
   - So, $j(n-1) = kp(p-1)$ for some k
   - Since $p \not| (n-1)$, we have $p|j$
   - So, only $(p-1)$ possible values for j,
     and $(p-1)$ possible values for a mod p^2
   - Proportion is then $\frac{p-1}{p^2-1} = \frac{1}{p+1} \leq \frac{1}{4}$

Strong pseudoprimes

1. For each composite $n > 9$:
   $|\{\text{strong pseudoprimes bases mod } n\}| \leq \frac{1}{4}\varphi(n) \leq \frac{n}{4}$

   Proof :(for the case where $n = pq$ and $a^t \equiv 1 \bmod n$)

   - $a^t \equiv 1 \bmod p$ and $a^t \equiv 1 \bmod q$
   - If g generates $\mathbb{Z}_p^*$ then $\exists j : a = g^j \bmod p$
     So, $jt \equiv 0 \bmod p - 1$
   - This only works for $\gcd(t, p-1) = \gcd(t, t') \leq t'$ values of j where $p - 1 = 2^{s'} t'$
   - Same thing $\bmod q = 1 + 2^{s''} t''$
   - So, proportion is at most $\frac{t' t''}{2^{s'+s''} t' t''} \leq \frac{1}{4}$ since $s', s'' \geq 1$

Strong pseudoprimes

1. For each composite $n > 9$:
   $|\{\text{strong pseudoprimes bases mod } n\}| \leq \frac{1}{4}\varphi(n) \leq \frac{n}{4}$

   Proof :(for the general case)

   - more prime factors $\Rightarrow$ more terms in the product, even better bound !
   - case $a^{2^r t} \equiv -1 \bmod n$: same approach, slightly refined :
     - count the $2^r t$-roots of -1 mod primes, as before
     - show that we cannot have $\gcd(t, t') = t'$ and $\gcd(t, t'') = t''$ (or n would have squares), so $t' t''$ bound is overstated

Strong pseudoprimes

1. For each composite $n > 9$:
   $|\{\text{strong pseudoprimes bases mod } n\}| \leq \frac{1}{4}\varphi(n) \leq \frac{n}{4}$

   Observations :

   - More factors $\Rightarrow$ more witnesses
   - $p - 1$ is a bigger power of 2 $\Rightarrow$ more witnesses

   When picking random values : high probability of detecting composite on first attempt !

Strong pseudoprimes

2. Under Extended Riemann Hypothesis ($\approx$ primes are well distributed), the first non strong pseudoprime base for composite n is $< 2\ln^2 n$

Proving primality
The $n-1$ method

Let $a,\ n \in \mathbb{N}^{>1}$
If $a^{n-1} \equiv 1 \pmod{n}$ but $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for every prime $q|(n-1)$ then n is prime.

Proof :

- $a^{n-1} \equiv 1 \pmod{n} \Rightarrow \mathrm{ord}(a)|n-1$
- $a^{(n-1)/q} \not\equiv 1 \pmod{n} \Rightarrow \mathrm{ord}(a)$ is not a strict divisor of $n-1$
- So a is of order $n-1$
- But $\mathrm{ord}(a)|\varphi(n)$
- $\varphi(n)$ can only reach $n-1$ when n is prime, so n must be prime

Proving primality
The $n-1$ method

Let $a,\ n \in \mathbb{N}^{>1}$
If $a^{n-1} \equiv 1 \pmod{n}$ but $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for every prime $q|(n-1)$ then n is prime.

Strategy :

- need a primitive root mod n
  but they are common $\approx n/(2 \ln \ln n)$
- Need the factors of $n-1$,
  hard in general, but we may *build* $n-1$ ourselves
- Need to prove that these factors are prime themselves
  A recursive proof might be needed
- But gives a proof in the end !

Proving primality
The $n-1$ method

Variant : Let $a,\ n \in \mathbb{N}^{>1}$ with a odd.
If $a^{(n-1)/2} \equiv -1 \pmod{n}$ and $a^{(n-1)/2q} \not\equiv -1 \pmod{n}$ for every odd prime $q | n-1$
then n is prime.

Proof :

- $a^{(n-1)/2} \equiv -1 \pmod{n} \Rightarrow a^{(n-1)} \equiv 1 \pmod{n}$
- $a^{(n-1)/q} \equiv 1 \pmod{n} \Rightarrow a^{(n-1)/2q} \equiv -1 \pmod{n}$
  Indeed, $(a^{(n-1)/2q})^2 \equiv 1$ and $(a^{(n-1)/2q})^q \equiv -1$
- So, $a^{(n-1)/2q} \not\equiv -1 \pmod{n} \Rightarrow a^{(n-1)/q} \not\equiv 1 \pmod{n}$

Proving primality
The $n-1$ method

Variant : Let a, $n \in \mathbb{N}^{>1}$ with a odd.
If $a^{(n-1)/2} \equiv -1 \pmod{n}$ and $a^{(n-1)/2q} \not\equiv -1 \pmod{n}$ for every odd prime $q | n-1$
then n is prime.

Example : 1279 is prime

- Claim that $1279 = 3^3 \cdot 71 + 1$ with 3 and 71 primes
- Look for a primitive root mod 1279. $a = 3$ works !
- Check that :
    - $3^{1278/2} \equiv -1 \pmod{1279}$
    - $3^{1278/(2\cdot 3)} \equiv 775 \not\equiv -1 \pmod{1279}$
    - $3^{1278/(2\cdot 71)} \equiv 498 \not\equiv -1 \pmod{1279}$
- Then prove that 3 and 71 are primes in the same way.

Factoring
Strategy 1 : Trial Division

$d \leftarrow 2$
while $d \leq \sqrt{n}$ **do**
    while $d | n$ **do**
        print d
        $n \leftarrow n/d$
    $d \leftarrow d + 1$

Complexity $\approx p$ divisions, with p smallest factor
Good for finding small factors !

Fermat method

If $n = u \cdot v$ is odd, then $n = a^2 - b^2$ where $a = \frac{u+v}{2}$ and $b = \frac{|u-v|}{2}$

Observations :

- $|u - v|$ is small if u and v are about the same size
  $\Rightarrow$ checking if $a^2 - n$ is a small b^2 for increasing a's might work !
- u and v do not need to be primes

Factoring
Strategy 2 : Fermat method

Search for a non trivial divisor of an odd n

for $\sqrt{n} \leq a \leq (n+9)/6$ **do**
  if $a^2 - n = b^2$ for an integer b **then**
    return $a - b$

Observations :

- Do not compute a^2 every time : $(a+1)^2 = a^2 + 2a + 1$
- Worst case is $n = 3p \Rightarrow a = (p+3)/2 = (n+9)/6$
  $\rightarrow$ Much worse than previous strategy !
  $\Rightarrow$ Try small factors first/in parallel
- Twist : try to factor kn with small k in parallel
  This may bring products of factors close to $\sqrt{kn}$

Pollard $p-1$

If $p|n$ and $p-1|M$
then $2^M \equiv 1 \pmod p$ and $p|\gcd(2^M-1, n)$

Ideas :

- Build M as a product of small factors and hope that $p-1|M$
- Do not compute 2^M-1 but $2^M-1 \bmod n$

Factoring
Strategy 3 : Pollard $p - 1$

$c \leftarrow 2 \qquad m \leftarrow 1$
$p \leftarrow$ list of primes $\leq B$
$a_i \leftarrow \max_j p_i^j \leq B$ for all i
for $1 \leq i \leq \text{length}(p)$ **do**
    for $1 \leq j \leq a_i$ **do**
        $c \leftarrow c^{p_i} \bmod n$
if $\gcd(c-1, n) \notin \{1, n\}$ **then**
    return $\gcd(c-1, n)$

Observations :

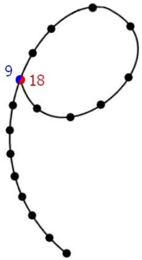
- Hope that the prime factors of *any* $p - 1$ are less than B
- Typically check gcd more often, in order to avoid trivial factors
- $B = 10^6$ gives 25% of 12 digit factors and 3% of 18 digit factors

Pollard ρ

Idea 1 :

1. Select x_1, ..., x_m in $\mathbb{Z}_n$
2. Search for (x_i, x_j) : $\gcd(x_i - x_j, n) \neq 1$

If p is smallest factor of n, then (x_i, x_j) exist for $m \approx \sqrt{p}$
But finding the (i, j) pair takes $\approx p$ tests



Idea 2 :

1. Compute $x_{i+1} = F(x_i)$ such that :
   $x_1 \equiv x_2 \pmod{p} \Rightarrow F(x_1) \equiv F(x_2) \pmod{p}$
2. Search (x_{2i}, x_i) : $\gcd(x_{2i} - x_i, n) \neq 1$

If p is smallest factor of n, then (x_{2i}, x_i) exist for $i \approx \sqrt{p}$

Eventual complexity is $\approx \sqrt{p} \approx \sqrt[4]{n}$

Factoring
Strategy 4 : Pollard ρ

With $F(x) = x^2 + a \pmod{n}$:

$a \xleftarrow{r} [1, n-1]$ $\quad$ $x_0 \xleftarrow{r} [0, n-1]$
$u \leftarrow x_0$ $\quad$ $v \leftarrow x_0$
while True **do**
  $u \leftarrow u^2 + a$
  $v \leftarrow v^2 + a$
  $v \leftarrow v^2 + a$
  if $\gcd(u - v, n) \notin \{1, n\}$ **then**
    return $\gcd(u - v, n)$
  if $\gcd(u - v, n) = n$ **then**
    Restart with new (a, x_0)