Last updated: January 5, 2006

9/22/2005

Review of Number System $\mathbb{Z}/_n$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	3	4	5	0	1	2
3	4	5	0	1	2	3
4	5	0	1	2	3	4
5	0	1	2	3	4	5

In $\mathbb{Z}/_6$, $3 + 4 = 1$

RSA Publuc Key Encryption

- Pick two large primes p and q. Let $n = pq$.
- Pick encryption exponent e.
- Publish e and n.

How to encode

Convert chunk of plaintext into integers x of range $0 \leq x < n$

$$E(x) = x^e \ \% \ n$$

How to decrypt

Decoding function is of form

$$D(y) = y^d \ \% \ n \qquad \text{What is } d?$$

Need $D(E(x)) = x$. That is, need $(x^e)^d \ \% \ n = x$. Or, $x^{ed} \ \% \ n = x$.

Euler's Theorem:

$$X^{\varphi(n)} \ \% \ n = 1$$

Where for $n = pq$, $\varphi(n) = (p-1)(q-1)$ Now, given e, let d be a multiplicative inverse of e mod $\varphi(n)$. Why does this d work?

Since d is a multiplicate inverse of $e \mod \varphi(n)$.

$$de = k\varphi(n) + 1 \qquad \text{(For some integer } k\text{)}$$

$$\begin{array}{rcl|l} D(E(x)) & = & (X^e)^d \ \% \ n & = X^{k\varphi(n)}X \ \% \ n \\ & = & X^{ed} \ \% \ n & = [X^{\varphi(n)}]^k X \ \% \ n \\ & = & X^{k\varphi(n)+1} \ \% \ n & = 1^k X \ \% \ n = X \end{array}$$

$\varphi(n)$ = number of integers i, $1 \leq i \leq n-1$ which are relatively prime to n.

i and n relatively prime means they have no common factors except 1, i.e. $gcd(i,n) = 1$

$\varphi(6) = 2$. 1, ~~2~~, ~~3~~, ~~4~~, 5. so, 2. Need to learn more about primes.

1. Unique factorization: Every integer factors into primes in essentially one way. e.x. $63 = 3 \cdot 3 \cdot 7$
2. Every polynomial with real coefficients factors into prime polyomials (irreducible polynomials) in essentially one way. e.x. $x^2 - 1 = (x-1)(x+1)$.

Look at unique factorization for integers

Euclid's Lemma Let p be a prime. If $p|(ab)$, then either $p|a$ or $p|b$.

> **Proof:** Suppose $p|a$. If $p \mid a$, done. If $p \nmid a$, then $gcd(p,a) = 1$.
>
> Use Euclidean Algorithm to write
>
> $$a = sp + ta \qquad \text{(for some int. } s \text{ and } t\text{)}$$
>
> $$b = spb + tab$$
>
> Now $p|spb$ and $p|tab$ (since $p|ab$), so $p|R.H.S.$, so $p|L.H.S.$, so $p|b$

How to get to unique factorization. Suppose we can write n as a product of primes in two ways:

$$n = p_1 p_2 p_3 p_4 \dots p_c$$

$$n = q_1 q_2 q_3 q_4 \dots q_d$$

Now $p_1|n$, so $p_1|q_1 q_2 \dots q_d$. So by Euclid's Lemma, $p_1|q_i$ for some i. So, $p_i = q_i$.

Goal is to write $1 = 13s + 104t$
$p = 13$, $a = 104$

$$\begin{aligned} 114 &= 8 \cdot 13 + 10 \\ 13 &= 1 \cdot 10 + 3 \\ 10 &= 2 \cdot 33 + 1 \end{aligned}$$

And then "backwards."

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 \\ &= 10 - 3 \cdot (13 - 10) \\ &= 4 \cdot 10 - 3 \cdot 13 \\ &= 4 \cdot (114 - 8 \cdot 13) - 3 \cdot 13 \\ &= 4 \cdot 114 - 35 \cdot 13 \end{aligned}$$

Same proof shows that polys with real coefficients factor in essentially only one way.

Division Alg.	$\Rightarrow$	Euclidean Algorithm
Euclidean Algorithm	$\Rightarrow$	Euclid's Lemma
Euclid's Lemma	$\Rightarrow$	Unique Factorization

Division algorithm: Given positive integer d, and integer n, we can write $n = qd + r$ for $0 \leq r < d$.

Division algorithm for polynomials: Given non-zero polynomial d and polynomial n, we can write $n = qd + r$ where degree of r is less than the degree of d.

9/27/2005

Example of RSA

$n = 5 \cdot 11 = 55$ ($n = pq$ product of two primes).
$e = 3$
publish $n = 5$, $e = 3$ (secret $p = 5$, $q = 11$).

$E(x) = x^3$. (ex. $E(41) = 41^3 \ \% \ 55 = 6$)

To decode: $D(x) = x^d \ \% \ 55$. We need d with $(x^e)^d \ \% \ 55 = x$.

> **Euler's Theorem**:
>
> $$X^{\varphi(n)} \ \% \ n = 1$$
>
> Where $\varphi(n)$ is the numer of integers i in range $a \leq i \leq n$ with $gcd(i, n) = 1$, provided $gcd(x, n = 1$.

$\varphi(5 \cdot 11) = (5 - 1)(11 - 1) = 4 \cdot 10 = 40$.
So, pick d to be a multiplicative inverse of 3 mod 40.
Thus $d = 27$.
Then $D(E(x)) \ \% \ 55 = (x^3)^{27} \ \% \ 55 = x^{81} \ \% \ 55 = (x^{40})^2 x \ \% \ 55 = x$

Square root attack on the RSA Cipher

Suppose you have a black box (oracle). You can feed it a number a and it spits out x where $x^2 \ \% \ n = a$. That is, suppose we can find square roots mod n. We don't know how to do this, but suppose we did.

Suppose we can find two square roots x and y of a with $x \neq \pm y \mod n$. (Seen an example of this: 1,4,11,14 are sqaure roots of 1 mod 15.)

$17^2 \ \% \ 55 = 14$. Suppose, $14 \rightarrow$ BLACK BOX $\rightarrow 27$.
Note, $17^2 \ \% \ 55 = 14$ but also $27^2 \ \% \ 55 = 14$. Now we have two really different square roots of 1, namely 17 and 27 (mod 55).

If x and y satisfy $x^2 \ \% \ n = y^2 \ \% \ n = a$, but $x \ \% \ n \neq \pm y \ \% \ n$.
Then, $n \nmid x - y$, $n \mid x + y$, but $n \mid x^2 - y^2$.

Explanation
Look at $\mathbb{Z}/_n$. Inside $\mathbb{Z}/_n$, we have $(\mathbb{Z}/_n)^*$ = all elements of $\mathbb{Z}/_n$ which have multiplicative inverses mod n = all elements i in $\mathbb{Z}/_n$ with $gcd(i, n) = 1$.

$\mathbb{Z}/_6 = \{1, 5\}$
$\mathbb{Z}/_7 = \{1, 2, 3, 4, 5, 6\}$
$\mathbb{Z}/_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$
Size of $(\mathbb{Z}/_n)^*$ is $\varphi(n)$

10/4/2005

homework, problem 3 hints: (a) Can Alice find $\varphi(n)$? And (b) Can she find some integer multiple of $\varphi(n)$? Use this multiple to find something "just as good". This means you can use it to decode.

Let's talk about $\mathbb{Z}/_n = \{0, 1, 2, \ldots, n-1\}$. Can add and multiply.

Also, $(\mathbb{Z}/_n)^*$ consists of all elemenest of $\mathbb{Z}/_n$ which have multiplicative inverses only considering mult.

Size of $(\mathbb{Z}/_n)^* = \varphi(n)$.

Given $a \in (\mathbb{Z}/_n)^*$, how many square roots does it have. (Square root means b with $b^2 = a \in \mathbb{Z}/_n$)
Answer depends on a.

Ex $a = 1$ in $\mathbb{Z}/_7$. Sqrts are 1, 6.
$a = 4$ in $\mathbb{Z}/_7$. Sqrts are 2, 5.
$a = 5$ in $\mathbb{Z}/_7$. Sqrts are nonexistant.

First, look at sqrt problem in $(\mathbb{Z}/_p)^*$ when p is prime.

Know (1) size of $(\mathbb{Z}/_p)^* = p - 1$. (2) If a has a sqrt b, it has another sqrt $-b$, so one sqrt implies at least 2 sqrts. (3) An element in $(\mathbb{Z}/_p)^*$ has at most 2 sqrts.

10/11/2005

from page 216+ of the textbook:

In $\mathbb{Z}/_p^*$, have primitive root g.
Then elements of $\mathbb{Z}/_p^*$ are:

$$\begin{array}{cccccccc} g^0, & g^1, & g^2, & g^3, & \cdots, & g^{p-2} \\ 1 & g \end{array}$$

Note that $g^{p-1} = 1$ by Euler's Theorem.
Half of the elements in $\mathbb{Z}/_p^*$ have no square roots and half have exactly two square roots.

Now work with two moduli, m and n, which are relatively prime.

$$\begin{aligned} x &= a \mod m \\ x &= b \mod n \end{aligned}$$

We want to solve this system.

Example

$$\begin{aligned} x &= 2 \mod 3 \\ x &= 1 \mod 5 \end{aligned}$$

Since m and n are relatively prime, can find s and t with $sm+tn = 1$. Now look at equation:

$$x_0 = a(tn) + b(sm) \mod mn$$

Claim Set of solutions to system is same as set of solutions to equation. First, let's show that any solution to equation is also a solutions to the system.

Given

$$x_0 = a(tn) + b(sm) \mod mn$$

Thus,

$$x_0 = a(tn) + b(sm) \mod m$$

Thus,

$$\begin{aligned} x_0 &= a(tn) \mod m \\ &= a(1 - sm) \mod m \\ &= a - asm \mod m \\ &= a \mod m \end{aligned}$$

In the same way, $x_0 = b \mod n$.

Back to our example...

$$\begin{aligned} x &= 2 \mod 3 \\ x &= 1 \mod 5 \end{aligned}$$

$m = 3$, $n = 5$, so $sm + tn = 2 \cdot 3 + (-1)5 = 1$.

$$\begin{aligned} x_0 &= 2(-5) + 1 \cdot 6 \mod 15 \\ &= -10 + 6 \mod 15 \\ &= -4 \mod 15 \\ &= 11 \mod 15 \end{aligned}$$

Checking...

$$\begin{aligned} 11 &= 2 \mod 3 \\ 11 &= 1 \mod 5 \end{aligned}$$

This gives all solutions to the system.

Find all solutions to $Z^2 = 1 \mod 15$. Look at:

$$z^2 = 1 \mod 3$$
$$z^2 = 1 \mod 5$$

$z^2 = 1 \mod 3$ has 2 solutions: 1 and 2
$z^2 = 1 \mod 5$ has 2 solutions: 1 and 4

Knit those together... Calculate $x_0 = a(tn) + b(sm) \mod 15 = a(-5) + b(6) \mod 15$

a	b	$-5a + 6b$
1	1	1
1	4	4
2	1	11
2	4	14

So, 1,4,11,14 are solutions.

10/13/2005

Example
Factor $x^2 - 9$ in two different ways.

Working mod 143. Note: $143 = 11 \cdot 13$.

Solution $x^2 - 9 = (x - b)(x + b)$ where $b^2 = 9$. Need to find all square roots of 9: 3 and -3, ?, ?

$x^2 = 9 \mod 11$
$x^2 = 9 \mod 13$

How do we put this together? Need $s \cdot 11 + t \cdot 13 = 1$
$13 = 11 + 2$
$11 = 5 \cdot 2 + 1$
So, $1 = 11 - 5 \cdot 2 = 11 - 5(13 - 11) = 6 \cdot 11 - 5 \cdot 13$

Get $6 \cdot 11 + (-5)(13) = 1$
$66 + (-65) = 1$

Solutions to $x^2 = 9 \mod 143$:

a	**b**	$\mathbf{66 \cdot a - 6 \cdot b} \mod \mathbf{143}$
3	3	3
-3	-3	-3
3	-3	-36
-3	3	36

Old obvious factorization is $x^2 - 9 = (x - 3)(x + 3)$. New is $x^2 - 9 = (x - 36)(x + 36)$

Example
Factor $x^2 - 4x + 5$ in two difference ways working mod 77. (note: $77 = 7 \cdot 11$) The obvious factorization: $x^2 - 4x + 3 = (x - 1)(x - 3)$.

Method 1:
complete the square: $x^2 + 4x + 3 = (x-2)^2 - 1 = [(x-2) - b] \cdot [(x-2) + b]$, where $b^2 = 1$.

Method 2:
$x^2 - 4x + 3 = (x-2)^2 - 1$
set $(x-2)^2 - 1 = 0$
$(x-2)^2 = 1$
$x - 2 = b$ with $b^2 = 1$
$x = 2 + b$ gives roots.

Method 3: Using the quadratic formula
$\frac{4 \pm \sqrt{16-4 \cdot 3}}{2} = \frac{4 \pm \sqrt{4}}{2} = \frac{4 \pm 2\sqrt{1}}{2} = 2 \pm 1$

Roots are: $b^2 = 1 \mod 7$
$b^2 = 1 \mod 11$
$11 = 7 + 4$
$7 = 4 + 3$
$4 = 3 + 1$
$1 = 4 - 3$
$= 4 - (7 - 4) = 2 \cdot 4 - 7$
$= 2(11 - 7) - 7$
$= 2 \cdot 11 - 3 \cdot 7$

"Knitting" solutions together then:

a	**b**	$\mathbf{22 \cdot a - 21 \cdot b} \mod \mathbf{77}$
1	1	1
-1	-1	-1
1	-1	43
-1	1	-43

Pick $b = 43$: $x^2 - 4x + 3 = [(x-2) + 43] \cdot [(x-2) + 43] = (x - 45)(x - 41) \mod 77$.

Euler's criteria for the existence of square roots

p odd prime, y relatively prime to p

$y^{\frac{p-1}{2}} = 1 \mod p \iff y$ has a square root.
$y^{\frac{p-1}{2}} = -1 \mod p \iff y$ does not have a square root.

If p is a prime with $p = 3 \mod 4$.

If y has a square root, then one square root is give by $y^{\frac{p-1}{2}} \mod p$.

Warning: If y does not have a square root, the above does not give a valid answer.

Example
$(\mathbb{Z}/_{11})^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$[(\mathbb{Z}/_{11})^*]^2 = \{1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 5, 5^2 = 3, 6^2 = 3, 7^2 = 5, 8^2 = 9, 9^2 = 4, 10^2 = 1\}$
Is 2 a square root? $2^5 = 32 = -1 \mod 11$, so no.
Is 3 a square root? $3^5 = 1 \mod 11$, so yes.
$5^3 = 125 = 4 \mod 11$, so 4 is a square root of 5.

$2^3 = 8$ but 8 is not a square root of 2!!

Issues with RSA

1. if we can finde square roots mode pq, then we can factor $n = pq$
2. need to find large primes p so we can produce RSA moduli pq
3. other ways of factoring large numbers

As n gets large, density of primes near n gets small. In fact, there are arbitrarily large gaps in sequence of primes.

Fermat's Theorem
If we know that p is a prime, then $yp - 1 = 1 \mod p$ (if y is relatively prime to p).
If for some y, $y^{p-1} \neq 1 \mod p$, then p is not prime.

If a number passes the Fermat test for base b, it is a Fermat pseudo-prime.

10/18/2005

Pseudo-Primes
A pseudo-prime is a number which passes some primality test. If the test fails, then the number is definitely composite. If it passes the test, then it is "likely" to be prime. "Likely" is very vague. We can figure out some probabilities for this.

First example of a primality test: **Fermat Test**:
Given n look at $2^{n-1} \% n$.

If $2^{n-1} \% n \neq 1$, n is definitely composite.
If $2^{n-1} \% n = 1$, n is "likely" to be prime. (It is a *Fermat Pseudoprime*)

What if n passes this test? Is n prime? Well, do the same test, but with a different base. Use Fermat Test base b. $(gcd(b, n) = 1)$.

Given n look at $b^{n-1} \% n$.

If $b^{n-1} \% n \neq 1$, n is definitely composite.
If $b^{n-1} \% n = 1$, n is "likely" to be prime.

Unfortunately, there are composite numbers which pass Fermat Test base b for every b. Ex: $n = 561$.

Euler Test Asks, Does $x^2 = b \mod n$ have a solution?

$$\left(\frac{b}{n}\right)_2 = \begin{cases} 0 & \text{if } gcd(b,n) \neq 1 \\ 1 & \text{if } x^2 = b \mod n \text{ has a solution} \\ -1 & \text{if } x^2 = b \cdots \text{ has no solutions} \end{cases}$$

Know if p is prime:

$$\left(\frac{b}{p}\right)_2 = b^{\frac{p-1}{2}} \mod p$$

(Euler's Criteria. p. 232)

Rk If n is not prime, $b^{\frac{p-1}{2}} \mod n$ is ???

Euler Test (base b)
If $\left(\frac{b}{n}\right)_2 \neq b^{\frac{p-1}{2}} \mod n$, then n is definitely composite. If $\left(\frac{b}{n}\right)_2 = b^{\frac{p-1}{2}} \mod n$, then n is likely to be prime.

Fact: If n is not prime, half the b's will show this. $(1 < b < n)$

Solovay-Strassen Test Want to know if n is prime or composite. Pick k random b's.

Apply Euler Test to n with each of these b's.

1. If n fails test for at least one b, then n is definitely composite.
2. If n passes test for all the b's, then n is prime with probability $1 - (\frac{1}{2})^k$

Ex: If $k = 10$, $1 - (\frac{1}{2})^{10} = 1 - \frac{1}{1000} \approx .999$
If $k = 20$, $1 - (\frac{1}{2})^{20} = 1 - \frac{1}{10^6} \approx .999999$

Miller-Rabin Test If it fails, definitely composite. If it passes, is prime with probability 3/4. (It is a *Strong Pseudoprime*)

n is the positive integer to be tested.
b is a random number $1 < b < n - 1$.

Write $n - 1 = 2^r \cdot m$ (with m odd). Do:
Compute $b_0 = b^m \% n$
If $b_0 = \pm 1 \mod n$, STOP: n is prime with probability 3/4. Otherwise, continue.
While $s < r$, compute $b_s = (b_{s-1})^2 \% n$.
If $b_s = -1 \mod n$, STOP. n is prime with probability 3/4.
If $b_s = 1 \mod n$ $(2 > 1)$, n is definitely composite.

Why is n definitely composite?

$$1 = b_s = (b_{s-1})^2 \mod n, \text{ where } b_{s-1} \neq \pm 1$$

So 1 has a square root (mod n) other than ± 1. Hence n is not prime. If none of $b_1, b_2, b_3, \ldots, b_{r-1}$ equals -1, n is definitely composite.

Ex $n = 9$, $n - 1 = 8 = 2^3 \cdot 1$, $r = 3$, $m = 1$. Pick $b = 5$.

$b_0 = 5^1 \% 9 \quad b_0 = 5$.
Is $b_0 = \pm 1 \mod 9$? No. Continue.
$b_1 = 5^2 \% 9 = 25 \% 9 = 7$.
Is $b_1 = \pm 1 \mod 9$? No. Continue.
$b_2 = 7^2 \% 9 = 49 \% 9 = 4 \neq \pm 1$.
Hence, 9 is definitely composite.

Ex $n = 11$, $n - 1 = 10 = 2 \cdot 5 \cdot 1$, $r = 1$, $m = 5$. Pick $b = 3$.

$b_0 = b^m = 3^5 \% 11 = 1$.
Is $b_0 = \pm 1 \mod 11$? Yes. STOP. n is probably prime.

10/20/2005

on page 269

Testing n, Using "random" b, write $n-1 = 2^r \cdot m$ for m odd.
$b_0 = b^m \ \% \ n$
If $b_0 = \pm 1$, Stop. n is probably prime. Otherwise continue.
Let $b_s = (b_{s-1})^2$,
If (for $s < r$), $b_s = -1 \ \% \ n$, Stop. n is probably prime.
If (for $s < r$), $b_s = 1 \ \% \ n$, Stop. n is definitely composite.

If none of $b_0, b_1, b_2, \ldots, b_{r-1} = \pm 1$, then stop: n is definitily composite.

Why
$b_0 = b^m$
$b_1 = (b^m)^2 = b^{2m}$
$b_2 = (b^2 m)^2 = b^{4m}$
$b_3 = (b^4 m)^2 = b^{8m}$o

In general, $b_i = b^{2^i m}$. Now suppose none of $b_0, b_1, b_2, \ldots, b_{r-1} = \pm 1$.
Look at $b_r = (b_{r-1})^2 = b^{2^r m} = b^{n-1}$.
If $b_r \ \% \ n \neq 1$, then n is composite by Fermat Test.
If $b_r \ \% \ n = 1$, then $1 = b_r = (b_{r-1})^2$ with $b_{r-1} \neq \pm 1$, so n is composite.

Example $n = 1001$, $b = 2$, $n - 1 = 1000 = 2^3 \cdot 125$

$b_0 = 2^{125} = 32 \ \% \ 1001 \quad 32 \neq \pm 1 \ \% \ 1001$ continue.

$2^2 = 4$
$2^4 = 16$
$2^8 = 256$
$2^1 6 = 256^2 \ \% \ 1001 = 471$

$b_1 = (32)^2 \ \% \ 1001 = 23 \neq \pm 1 \ \% \ 1001$ continue.
$b_2 = (23)^2 \ \% \ 1001 = 529 \neq \pm 1 \ \% \ 1001$ continue.

1001 is definitely composite.

[section on fast modular exponentiation. page 207.]

On test Two

1. Stuff from exam 1
2. Ch. 10: RSA cipher & Diffie-Hellman
3. Ch. 12: Fermat's Theorem (12.1) [Special case of Euler's Theorem]
4. Ch. 13: §13.2 & 13.3. Know how to solve $x^2 = a \mod pq$ and
   $x = a \mod p$
   $x = b \mod q$
   Also, Euler's Theorem & Euler's Criterion for square roots.
5. Recently

   12.5 Exponential Algorithm

   12.6 Square Roots mod p, $p = 3 \ \% \ 4$

13.5 Square Root Oracle

6. And Ch. 16

16.1 Fermate Pseudo-primes

16.3 Euler Pseudo-primes

16.4 Solavay-Strassen

16.6 Miller-Rabbin

Test Two

Remarks Motivated by RSA

Discussion About Primes

1. There are an infinite number of primes.
   Proof Suppose we had a list $P_1, P_2, P_3, \ldots, P_N$ of all the primes. Let
   $M = P_1P_2 \cdots P_N + 1$ If M is prime, then it is a new prime not on the list. On the other hand, if M is not prime, it must have a prime facotr p. So, p is prime, $p \mid M$. Could p be P_1? No. $p_1 \nmid M$. Could p [Board erased]...

2. There are arbitrary large gaps between primes.
   Explanation Let $M = n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots n$.
   $M + 2 = n! + 2$ is divisible by 2.
   $M + 3 = n! + 3$ is divisible by 3.
   $M + 4 = n! + 4$ is divisible by 4.
   $\vdots$
   $M + n = n! + n$ is divisible by n.

   String of $n - 1$ consecutive integrers, none of which is prime.
   Illustration Find 4 consecutive non-prime integers. Using above,
   $5! + 2 = 122$
   $5! + 3 = 123$
   $5! + 4 = 124$
   $5! + 5 = 125$

   Prime Number Theorem: $f(x) \sim g(x)$ means $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$
   Warning: $f(x) \sim g(x)$ does not necessarily mean $\lim_{x\to\infty} f(x) - g(x) = 0$

   Let $\Pi(x) = \#$ of primes $< x$. Then $\Pi(x) \sim \frac{x}{lnx}$ $\quad \left[\frac{\Pi(x)}{x} \sim \frac{1}{lnx}\right]$

   Example: How many primes are there $< 10,000$?

$$\frac{10000}{ln10000} \cong \frac{10000}{92} \approx 1086$$

   In fact, $\Pi(10000) = 1221$.

Motivated by Diffie-Hellman And ElGamil. (Related to Structure of $(Z/_n)^*$ and discrete logs)
$(Z/_n)^*$ is an example of a *group*. What is a group? A group is a set G together with an operation * satisfying:

1. $(a * b) * c = a * (b * c)$
2. There is an element e in G (called the identity) such that $g * e = g = e * g$ For every g in G.
3. For each a in G, there is a b in G such that $a * b = e = b * a$. (The inverse).

Remark If $a * b = b * a$ for all a and b in G, we say that the group is "commutative" or "abelian".

Ex

1. $\mathbb{Z}$ = The integers. Operation is addition. $e = 0$. inverse of a is -a.
2. $(Z/_n)^*$ operation is multiplication mod n. $e = 1$. Inverse of a is multiplicative inverse of $a \mod n$.
3. $Z/_n$. operations is addition mod n.

The above are all abelian.

Example of a group which is not abelian: M_2 = All 2x2 invertible matrices.
(invertible $\iff$ has an inverse $\iff$ has a non-zero determinate.)
Operation is matrix multiplication.

Another non-abelian group: All rotation about origin in $\mathbb{R}^3$. Operation is composition of rotation.

Definition A group G is called cyclic if there is a g in G such that every element h innn the group is of the form g^n for some n.

11/8/2005

Looking at $(\mathbb{Z}/_5)^* = 1, 2, 3, 4$. * is multiplication mod 5. $e = 1$.

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Looking at $\mathbb{Z}/_5 = 0, 1, 2, 3, 4$. * is addition mod 5. $e = 0$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Definition G is *Cyclic* if there is an element g in G such that g^n can fill up G (like primitive root).

Is $\mathbb{Z}/_5$ cyclic?
Try $g = 1$.
$g * g = g + g = 2g = 2$
$g * g * g = g + g + g = 3g = 3$
$g * g * g * g = g + g + g + g = 4g = 4$
$g * g * g * g * g = g + g + g + g = 4g = 4$
Yes, Cyclic.

More examples of Groups:

Rotations of a square:

1. $R_{90} \equiv 90^\circ$ counter-clockwise.
2. $R_{180} \equiv 180^\circ$ counter-clockwise.
3. $R_{270} \equiv 270^\circ$ counter-clockwise.
4. $R_0 \equiv$ identity.

[Blah, Blah, Blah. Lots of group stuff]

11/10/2005

Groups

Let G be a group.

Definition H is a *subgroup* of G if H is a subset of G, and H is a group (using operation in G)

Examples

1. G = $\mathbb{Z}$. H = $2\mathbb{Z}$ (even integers). Yes, H is a subgroup of G.
2. G = $\mathbb{Z}$. H = odd integers. *Not* a subgroup. If you add two odd integers, you get an even integer.
3. G = $\mathbb{Z}$. H = non-negative integers = $0, 1, 2, 3, \cdots$. *Not* a subgroup. No inverses.
4. G = all symmetries of equilateral triangle. H = All rotations together with identity. H is a subgroup of G.
5. G = All symmetries of equilateral triangle. H = all flips, together with identity. *Not* a subgroup: you can combine two flips to get a rotation.

If g is an element of G, then $\langle g \rangle$ is the subgroup of G generated by g: That is:

$$\langle g \rangle = \{g, g^2, g^3, g^4, \ldots\} = \{g^n : n \in \mathbb{Z}\}$$

Notation: g^{-1} means inverse of g. g^{-2} means inverse of g^2. ...

Example $(\mathbb{Z}/_{11})^*$ (has 10 elements)
$\langle 2 \rangle = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\} = (\mathbb{Z}/_{11})^*$
$\langle 3 \rangle = \{1, 3, 9, 5, 4\}$

Example $(\mathbb{Z}/_{15})^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ (has 8 elements)
$\langle 2 \rangle = 1, 2, 4, 8$
$\langle 4 \rangle = 1, 4$

By the *order* of a group G, we mean the number of elements in G. Write $|G|$

$\langle 2 \rangle = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\} = (\mathbb{Z}/_{11})^*$
$\langle 3 \rangle = \{1, 3, 9, 5, 4\}$

Theorem *(Lagrange)* If G is a finite group, and H is a subgroup of G, then the order of H divides order of G.

11/15/2005

Let $g \in G$
Definition: Order $G = |G|$ = size of G Def: Order $g = |\langle g \rangle|$ = smallest positive integer such that $g^n = e$, the identitiy.

Example: $(\mathbb{Z}/_7)^*$ $\quad |(\mathbb{Z}/_7)^*| = 6$

What is the order of 2 in $(\mathbb{Z}/_7)^*$?

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8 = 1$

Answer: 3

Theorem: If $g \in G$, then $|g|$ divides $|G|$. Proof: $|g| = |\langle g \rangle|$, and by lagrange's Theorem, the order of a subgroup divides the order of a group.

EX: what are the possible orders of elements in $(\mathbb{Z}/_{107})^*$?

Solution: $|(\mathbb{Z}/_{107})^*| = 106$, $(106 = 2 \cdot 52)$ so possible orders of elements are: 1, 2, 53, 106

Theorem: If $g \in G$, and $|G| = n$, then $g^n = e$

Proof: Let $d = |g|$, know $d|n$. Then $g^n = (g^d)^{n/d} = e^{n/d} = e$

Correlary: *(Another proof of Euler's Theorem)* If x is relatively prime to p, then $X^{p-1} = 1 \mod p$. (p prime.) Proof: $|(\mathbb{Z}/_p)^*| = p-$, so by previous theorem, $X^{p-1} = 1 \mod p$.

Look at discrete logs:

Given b, Primitive root mod p. Given a, want to solve $b^\ell = a \mod p$.

One attack Let G be a cyclie group. Let $n = |G|$. Let $m = \lfloor \sqrt{n} \rfloor$

Given b and a in G, know b is a generatory.

$\langle b \rangle = G$. Find ℓ such that $b^\ell = \ell$.

Example Solve $43^\ell = 2 \mod 31$. Don't know ℓ, but in any case ℓ can be written as

$$\ell = mi + j \qquad \begin{matrix} 0 \leq j < m \\ 0 \leq i < m \end{matrix}$$

Then $z = b^\ell = b^{mi+j} = b^{mi} b^j$.

Rewrite: $a(b^{-m})^i = b^j$

So compute b^j for $j = 0, 1, 2, \ldots, m-1$. Then computer, in turn, ab^{-m}, ab^{-2m},ab^{-3m}. After each computations, compare with list of powers of b.

Example Solve $3^\ell = 2 \mod 31$. $b = 3$, $a = 2$

$m = \lfloor\sqrt{30}\rfloor = 5$ compute powers of b:

j	0	1	2	3	4
3^j	1	3	9	27	19

Now compute:
$2 = 2$
$2 \cdot 3^{-5} = 2 \cdot 6 = 12$
$2 \cdot 3^{-10} = 2(3^{-5})^2 = 12 \cdot 6 = 10$
$2 \cdot 3^{-15} = 2(3^{-5})^3 = 10 \cdot 6 = 29$
$2 \cdot 3^{-20} = 2(3^{-5})^4 = 29 \cdot 6 = 19$

$2 \cdot 3^{-20} = 3^4$.
$2 = 3^{24}$.
$\ell = 24$

Exponential Notation in Groups

G is any group, g is an element in G.

Definition $g^0 = e$, $g^1 = g$, $g^2 = g \times g$. And in general $g^k = g \times g \times \cdots \times g$.

g^{-1} = inverse of g
$g^{-2} = (g^{-1})^2$
$g^{-k} = (g^{-1})^k$

11/17/2005

Pollard – Find Discrete Logs – Factor – (depends on "Birthday Paradox")

Use Pollard's Method to factor 5893

Given n (# we want to factor)
Start with $x = 2$, $y = x^2 + 1 = 5$.

Compute $gcd(x - y, n)$

If $1 < gcd < n$, Done. We have afound a factor of n.

If $gcd(x - y, n) = n$, Method fails, reinitialize.

If $gcd(x - y, n) = 1$, Replace x with $q^2 + 1$, y with $(y^2 + 1)^2 + 1$. Repeat

x	y	$x - y$	$gcd(x - y, 5893)$
2	5	-3	1
5	677	-672	1
26	2756	-2730	1
677	2844	-2167	1
4569	1000	3569	83

Found a factor of 5893, namely 83.

Birthday Paradox

Room with n People. $P(n) = 2$ (or more) people have the same birthday.
$P(35) \approx 81.4\%$

$P(23) \approx 50.7\%$

Calculate $P(n)$

$P(1) = 0$

$P(2) = 1/365$

$P(3) = 1 - P(\text{All birthdays distinct}) = 1 - (\frac{364}{365}) \cdot (\frac{363}{365}) \approx 0.008$

$P(4) = 1 - (\frac{364}{365}) \cdot (\frac{363}{365}) \cdot (\frac{362}{365}) \approx 0.016$

So,

$$P(n) = 1 - P(\text{All birthdays distinct}) = \left(\frac{364}{365}\right) \cdot \left(\frac{363}{365}\right) \cdots \left(\frac{365-(n-1)}{365}\right)$$

In general, if we have an experiment with N equally likely outcomes, And we perform experiment n times, Then $P(n)$, probability that two or more outcomes are the same, is

$$P(n) = \left(\frac{N-1}{N}\right) \cdot \left(\frac{N-2}{N}\right) \cdots \left(\frac{N-(n-1)}{N}\right)$$

$P(n)$ becomes $> \frac{1}{2}$ for moderately small n. (roughtly $n > \sqrt{N}$)

What does this have to do with Pollard's Method?

Given n, set $x = 2$, $y = x^2 + 1$.

x_1	2	y_1	5
x_2	5	y_2	677
x_3	26	y_3	2756
x_4	677	y_4	2844
x_5	4569	y_5	1000
x_6	2756	y_6	...

Note: $x_{2i} = y_i$ Why? Surely, $x_2 = {x_1}^2 + 1 = y_1$. If we know $x_{2i} = y_i$, Let's evaluate x_{2k}.

$$x_{2k} = (x_{2k-1})^2 + 1 = \left((x_{2k-2})^2 + 1\right)^2 + 1 = \left((y_{k-1})^2 + 1\right)^2 + 1 = y_k$$

(Note: proof by induction)

All of our calculates can be done (should be done) mod n.

Suppose d is a factor of n, (ww don't know at the moment what d is). Pretend we reduce all x_i (or all y_i) mod d. Assume this produces random numbers, mod d. How long will it take for the probability that 2 x's are equal mod d is $\geq 1/2$? Answer: about $\sqrt{d}$.

Example Suppose $x_8 \equiv x_{14} \mod d$. But x's are periodic. Can find two x's such that $y_i = x_{2i} = x_i \mod d$. Refer to §24.1

Pollard's Rho Method: *(For Factoring)* n given. Want to factor n. Set $x = 2$, $y = x^2 + 1$.

Look at $gcd(x-y,n)=g$. If $1<g<n$, found factor of n. Otherwise, Replace x by x^2+1, y by $(y^2+1)^2+1$.

Example: $n=45811$

x	y	$x-y$	$gcd(x-y,45811)$
2	5	-3	1
5	677	-672	1
26	2590	-2569	1
677	11289	-2167	1
220	1000	-10612	1
2590			1
19695			1
11289			1
41131			1
4743	30180	-25437	61

So, $gcd(-25437,45811)=61$.

Note, this is all done modulo 45811

Why does this work? Suppose (secretly) that d is a fator of n. If we do calculations mod d, how long will it take to get a repear ($x_j=x_i \mod d, i<j$)? Might take d steps, but probability of a repeat is greater than $a/2$ for about $\sqrt{d}$ steps (birthday paradox).

Why does this mean that $gcd(x_k-y_k,n)>0$ for some small k. Showing by example:

Supposed that $x_{15}=x_{11} \mod d$. Then $x_{16}=x_{12}$, $x_{17}=x_{13}$, etc. That is, if the difference in the subscripts is 4, the x's will be the same, provided subscripts are ≥ 11. Similarly, if the difference in subscripts is a multiple of 4, the x's will be the same. Then $x_{24}=x_{12}$. So, $y_{12}=x_{12} \mod d$, so $gcd(x_{12}-y_{12},n)$ will be at least d.

Some Review

G is a group, g is an element of G. Look at $\{g^0=e,g^1=g,g^2,g^3,g^4,\ldots\}$

Question 1: Must there be a repeat? ($g^j=g^i$, $i\neq j$) No. G = positive reals, using multiplications, g = 2.

Question 2: If G is finite, must there be a repeat? Yes, there are only a finite number of possibilities for each g^i, so eventually we will get a $g^j=g^i$, for some $i\neq j$.

Question 3: Suppose there is a repeat? Could first repeat be $g^{15}=g^{11}$? No.
$g^{15}g^{-11}=g^{11}g^{-11}$
$g^4=g^0$

Lesson: first repeat must be $g^k=e$, k some non-negative integer.

If g is a primative root in $(\mathbb{Z}/_{101})^*$, what is k? $k=100$. If g is a primative root, then everything must be covered before there is a repeat.

If g is some element in $(\mathbb{Z}/_{101})^*$ and k is smallest positive number with $g^k=1$, what are the possibilities for k? k must be a divisor of $|(\mathbb{Z}/_{101})^*|=100$ So, 1, 2, 4, 5, 10, 20, 25, 50, 100 are all posibilities.

On test three (From email)

Since we haven't had much HW lately, I have been asked to list some problems and sections relevant to the third midterm.

- **16.6** Miller-Rabin Test – You did have HW on this; if you want more exercises, try 16.6.01 and 16.6.06
- **Groups** Chapter 17 – We spent a fair amount of time discussing groups. One reason we did this was so we could better understand the structure of $(\mathbb{Z}/_p)^*$, and we need to understand $(\mathbb{Z}/_p)^*$ so we can use discrete logs in ElGamil and Diffie-Hellman. There will not be any proofs on the exam, but you may have to analyze various situations, as you have done on previous exams.

  Here are some specific problems to work on:

  17.1: 03,04 17.2: 01,05,06,07,09 17.6: 05,09 (don't so this by checking lot's of cases; there is a short, simple explanation),10
- **24.1** Pollard's Rho method for factorization– 24.1: 01,02,03
- **27.1** Baby step Giant step for discrete logs – 27.1: 01,09,12

In connection with Pollard's Rho method, we discussed the birthday paradox. See pages 28-30. Suppose there is an experiment which has N equally likely outcomes. If we perform the experiment n times, we want to know the probability that two or more outcomes will be the same. The "paradox" is that even when n is much smaller than N, the probability is quite high. For example, if the experiment is picking a person and asking their birthday ($N = 365$), when $n = 23$ the probability of two people having the same birthday is already more than 1/2.

11/29/2005

Pollard's Rho Method for Discrete Logs: Working mod p (prime), given b and c, want to find L such that $b^L = c$. ($L = \log_b c$)

Say working in some cycle group G (Recall that $(\mathbb{Z}/_p)^*$) is cyclic)

Divide G into three non-overlapping parts S_1, S_2, S_3.

Define a function $f : G \to G$

$$f(x) = \begin{cases} cx & \text{if } x \in S_1 \\ x^2 & \text{if } x \in S_2 \\ bx & \text{if } x \in S_3 \end{cases}$$

Start with $x_0 = c^{m_0} b^{n_0}$

Let $x_1 = f(x_0)$, $x_2 = f(x_1)$, $\ldots$, $x_i = f(x_{i-1}) = c^{m_i} b^{n_i}$

"Pretty soon" (Birthday paradox) get $x_i = x_j$ for some $i \neq j$. Then get $c^{m_i} b^{n_i} = c^{m_j} b^{n_j} \Rightarrow b^{n_1 - n_j} = c^{m_j - m_i}$. Find multiplicative inverse t of $m_j - m_i \mod |G|$

$(b^{n_i - n_j})^t = (c^{m_j - m_i})^t$
$b^{(t)(n_i - n_j)} = c$ So $L = (t)(n_i - n_j)$

Example $p = 38$. 2 is a primitive root, so 2 generate cyclic group $(\mathbb{Z}/_{83})^*$ of order 82. Then $2^2 = 4$ generates a cyclic subgroup G of $(\mathbb{Z}/_{83})^*$, of order 41. Note: $x \in G \iff x$ is a square mod 83.

Goal: given c, (a square mod 83), solve $4^L = c$.

Example Take $c = 3$ (ok that 3 is a square mod 83). So $4^L = 3$ does have a solution.

Start with $x_0 = 3^{m_0}4^{n_0} = 1$. That is, take $m_0 = 1$, $n_0 = 1$.

Looking for i and j, with $x_i = x_j$.

Instead, define sequence $\{Y_i\}$ along with sequence $\{X_i\}$ by rule

$$y_0 = 1$$

$$y_i = f(f(x_{i-1})) = X_{2i}$$

$X = 3^{m_x}4^{n_x}$
$Y = 3^{m_y}4^{n_y}$

Divide G into three pieces:
$S_1 = \{1, 4, 7, \ldots\} \cap G \quad f(x) = cx$
$S_2 = \{2, 5, 8, \ldots\} \cap G \quad f(x) = x^2$
$S_3 = \{3, 6, 9, \ldots\} \cap G \quad f(x) = bx$ Fill out the table until we get an x value equal to a y value.

x	m_x	n_x	Y	m_y	n_y
1	0	0	1	0	0
3	1	0	12	1	1
12	1	1	26	1	3
48	1	2	48	2	7

Doing some of the computations for the above table:
$Y_1 = 12 = 3^1 \cdot 4^1$
$Y_2 = f(f(Y_1))$. First $f(Y_1) = f(12) = f(3^1 \cdot 4^1) = 3^1 \cdot 4^2$ (12 in S_3) $= 48$. Then, $Y_2 = f(48) = f(3^1 \cdot 4^2) = 3^1 \cdot 4^3 = 26$

So, $3^1 \cdot 4^2 = 48 = 3^2 \cdot 4^7$. Then, $4^{-5} = 3$. Want 4 to a positive power:
$2^{82} = 1 \mod 83$
$4^{41} = 1 \mod 83$ So, $3 = 4^{-5} = 4^{-5} \cdot 4^{41} = \boxed{4^{36}}$

12/6/2005

Implementation of RSA

Say we want to use two primes of about 100 digits.

100 digits $\approx$ 333 bits. MSB (least significant bit) is 1, because otherwise it woulnd't be 333 bits. LSB (least significant bit) is 1, otherwise it would be an even number and not prime. So, we need to pick 331 bits at "random."

How many ways to do this? $2^{331} \approx 2 \cdot 10^{99}$ (many). So we get a 333 bit number N. Need to know if it's prime. Use a primality test on this number. Miller-Rabin is in common use. If N not prime, test $N+2$, $N+4$, $N+6$, until you get prime p.

How long will this take? How likely is a large number to be prime?

Prime Number Theorem

Let $\Pi(x)$ be the number of primes $\leq x$. Then,

$$\frac{\Pi(x)}{x} \sim \frac{1}{\ln x}$$

(We say $f(x) \sim g(x)$ ($f(x)$ assymptotic to $g(x)$) if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.)

Example If $x = 10^{100}$,

$$\frac{\Pi(x)}{x} \sim \frac{1}{\ln 10^{100}} = \frac{1}{100\ln(10)} = \frac{1}{230}$$

That is, about $\frac{1}{230}$ of the numbers $\leq 10^{100}$ are prime.

Do Better: Estimate number of primes between x and $x + \Delta x$. $(= \Pi(x+\Delta x) - \Pi(x))$

Now, $\frac{\Pi(x)}{x} \sim \frac{1}{\ln x}$, so $\Pi(x) \sim \frac{x}{\ln x}$. Thus,

$$\Pi(x+\Delta x) \cong \Pi(x) + \Delta x \left(\frac{x}{\ln x}\right)'$$

Equivalent to:

$$\frac{\Pi(x+\Delta x) - \Pi(x)}{\Delta x} \cong \left(\frac{x}{\ln x}\right)'$$

$$\left(\frac{x}{\ln x}\right)' = \frac{x'\ln x - x(\ln x)'}{(\ln x)^2} = \frac{\ln x - x/x}{(\ln x)^2} = \frac{\ln x - 1}{(\ln x)^2}$$

Thus,

$$\Pi(x+\delta x) \cong \Pi(x) + \frac{\Delta x}{\ln x}$$

This says, between x and $x+\Delta x$, there are approximately $\frac{\Delta x}{\ln x}$ primes. That is, in this rance about $\frac{1}{\ln x}$ of number are prime.

In range, 10^{100} to $10^{100} + \Delta x$, about $\frac{1}{\ln(10^{100})} \cong \frac{1}{230}$ of number are prime.

How many times should you apply Miller-Rabin test to any number until you are "Sure" it is prime? apply once and get "Probably prime," chance of error $\approx \frac{1}{4}$. Apply k times, chance of error $= \frac{1}{2^{2k}}$

Digital Signatures (in RSA context)

Be sure that source of message is who it claims to be.

You have P and Q (private). Publish n ($= PQ$) and encryption exponent e. Only you know decryption exponent d.

$\text{Plaintext} \xrightarrow{e} \text{Cyphertext} \xrightarrow{d} \text{Plaintext}$

Goal: when I send you a message, I want to tack on a "digital signature" so you will know that only I could have sent the message.

I have my own RSA implementation with public encryption exponent $\bar{e}$ and private decryption exponent $\bar{d}$.

Signature is $\bar{d}(H(\text{plaintext}))$ for hash function H

12/8/2005

Existance of Primative Roots on $(\mathbb{Z}/_p)^*$, p prime.

Look at polynomial (with $(\mathbb{Z}/_p)^*$ coefficient)

$$f(x) = X^{p-1} - 1$$

1. For every $b \in (\mathbb{Z}/_p)^*$, $b^{p-1} = 1$ (Euler). so b is a root of $f(x)$.
2. $X^{p-1} - 1$ has at least $p - 1$ roots
3. Finished taking notes for class on paper...