CIS 3362 10/20/25

last number theory topic

factorization algorithms

lots of complicated algorithms out there (quadratic sieve)

default: is brute force, just try division (mod) with each integer.

Fermat Factoring

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

true if n is odd product of 2 odd ints.

31×17

$(24+7)(24-7)$

$= 24^2 - 7^2$

$n = 527$

$x^2 = n + y^2$

$x^2 = 527 + y^2 \rightarrow x^2 - 527 = y^2$

$x^2 - n = y^2$

$\sqrt{527} = 22.\ldots$

x	$x^2 - 527$ y^2	is this a perfect sq
23		

plug in successive values for x.

x	x^2	$x^2 - 527$ y^2	is per sq
23	529	2	no
24	576	49	yes ✓

$576 = 527 + 49$

$24^2 - 7^2 = 527$

$527 = (24+7)(24-7)$

31×17

217

31

527

tends to be better if both prime factors are "close" to each other.

Pollard-Rho Factorization (factoring 1)

$a_0 = 2$ create a sequence

$a_i = \left((a_{i-1})^2 + 1 \right) \bmod n$

2, 5, 26, 677, ...

if $n = p \times q$
repeat mod p with $p-1$ steps to 1
repeat mod q within $q-1$ steps to 1.

if I ever find i and j such that

$\gcd(a_i, a_j) > 1$

then that gcd has to be p or q or n.

WORKS sometimes + fails other times
Fermat always works but could be insanely slow.

$a = 2$, $b = 2$

```
while (true) {
    a = (a*a+1) % n
    b = (b*b+1) % n
    b = (b*b+1) % n
    ~~if (gcd(a,b) > 1)~~ gcd(a-b, n)
    tmp = ~~gcd(a,b)~~
    if (tmp > 1 and tmp < n) return tmp, n/tmp
}   if (tmp == n) return failed
```

This works better than Fermat

1) Show code

2) Talk about QUIZ

QUIZ

1) Calculator, still show work

2) Number Theory

Prime Factorization

Euler Phi Function + formula

Fermat Thm if $\gcd(a,p)=1$, $a^{p-1} \equiv 1 \bmod p$

Euler's Thm if $\gcd(a,n)=1$, $a^{\phi(n)} \equiv 1 \bmod n$

Discrete Log Problem

Primitive Roots / Generators

Miller-Rabin Primality Test

Fast Mod Expo

Showed Divide Conquer Discrete Log Soln in $\sim O(\sqrt{p})$ time. Factoring Algs

3) 1 Sheet of Notes ($8.5'' \times 11''$ typed or written both sides)

~~8x5~~

$$43^{3002} \bmod 101$$

By fermat's thm, $43^{100} \equiv 1 \bmod 101$ since 101 is prime.

$$43^{3002} = 43^{3000} \times 43^2$$
$$= (43^{100})^{30} \times 43^2$$
$$\equiv 1^{30} \times 43^2 \equiv 1849 \equiv 31 \bmod 101$$