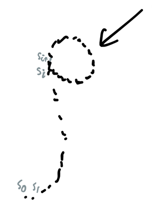
Lecture 13

Tuesday, 18 October 2022 13:30

Pollard's rho method for factorization

Let prime p divide n. We want: a factor of n $\longrightarrow$ at least split off p or a factor containing p



$\sqrt{p}$ till we meet,

we want a step function that meets mod p

if $s_i \equiv s_j \mod p$, then $\gcd(\underbrace{s_i - s_j}_{\equiv 0 \bmod p}, \underset{\equiv 0 \bmod p}{n}) \equiv 0 \mod p$

Bad case: $\gcd = n \longrightarrow$ no factor

Otherwise, get a proper factor divisible by p.

Step function $f(s_i) = s_{i+1}$ is defined mod n; this is compatible with mod p, because p divides n.

$f(s) = cs^2 + d \qquad \mod n$

for some $0 < c, d < n$

Floyd's cycle finding method makes us compare s_{2i} and s_i.

see slides: $(\rho_1 - \rho_2)(\rho_2 - \rho_4)\dots$

no point in computing gcd's after each step, instead compute one gcd with the product of all differences

For $i < \sqrt{p}$ ← we have some idea how big p is

$i < B$

$s_{i+1} \equiv cs_i + d \mod n$

$s_{2(i+1)} \equiv c\,(c\,s_{2i}^2 + d)^2 + d \mod n$

$s \leftarrow s \cdot (s_{2(i+1)} - s_{i+1}) \mod n$

$\gcd(s, n)$ ← computes $s \bmod n$; therefore, we can compute mod n here already

starting values	$s = 1$, $s_0 =$ starting value

Iterate with new s_0, c, d on each factor that is not prime

If we don't factor, increase B, this means there are no small primes p.

If the gcd is n, decrease B ← then we have that more than one factor of n is included in the product

Big factorization (Dixon or number-Field Sieve) need to factor auxiliary numbers; want only smooth ones $\hat{=}$ lots of small factors to find matches

For each do trial division up to B_1, then Pollard-rho up to B_2, then $p-1$ & ECM.

Discard if not enough progress (early abort)

"Sieve" in NFS refers to small primes found by sieving rather than trial division.

Auxiliary numbers have some known spacing, so can efficiently divide out small primes from all numbers at the same time

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

13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~

we now have factored completely

2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24

Use Pollard-rho on remaining ones (and primality test on 7, 11, 13, ...)

Coppersmith's method