Integer factorization

$$n\,(>1) = \prod_{i=1}^{k} p_i^{\alpha_i} \quad (\text{F.T.A.})$$

I.F. Algo

Deterministic — Prob.

Forms & Prop. of integers Classification

General purpose factoring algo.

— The running time depends mainly on the size of n (and is not strongly dependent on the size of the factor p found)

Examples Algo

1. Lehman's method (1974) — Worst case running time bound $O(n^{1/3+\epsilon})$

2. Euler's factoring method ~~(1996~~)
   deterministic running time $O(n^{1/3+\epsilon})$

3. Shank's SQUare FOrm factorization method (SQUFOF) (1975)

   $O(n^{1/4})$

(4) The FFT based factoring method (1974, 1976/1997)
Pollard & Strassen

deter. run.time $O(n^{1/4+\epsilon})$

(5) The Lattice based factoring method (1997)
Coppersmith $O(n^{1/4+\epsilon})$

(6) Shanks' class group method (1971)
assuming ERH $O(n^{1/5+\epsilon})$

(7) Continued fraction method (CFRAC) (1975)
under plausible assumptions (U.P.A.) has exp. run. time

Verify!

$$O(\exp(c\sqrt{\log n \log\log n})) \stackrel{?}{=} O(n^{c\sqrt{\log\log n/\log n}})$$

c (usually) $= \sqrt{2} = 1.414213562$

(8) Quadratic Sieve / Multiple Poly. Quad. Sieve (1985)
(QS/MPQS)
U.P.A.

Verify!

$$O(\exp(c\sqrt{\log n \log\log n})) = O(n^{c\sqrt{\log\log n/\log n}})$$

$$c = \frac{3}{2\sqrt{2}} \simeq 1.060660172$$

(9) Number Field Sieve (NFS) (1993)

U.P.A. exp. runn. time

$$O\left(\exp\left(c\sqrt[3]{\log n}\,\sqrt[3]{(\log\log n)^2}\right)\right)$$

$c = (64/9)^{1/3} \simeq 1.922999427$

if GNFS (a gen. ~~version~~ version of NFS) is used to factor

whereas

$c = (32/9)^{1/3} \simeq 1.526285657$

if SNFS (a special version of NFS) is used to factor special integers $n = r^e \pm s$

r, s <<< small

$r > 1$ & e is large.

$\boxed{\text{asymp. faster algo}}$

$\boxed{\text{Special purpose factoring algos}}$

The runn. time depends mainly on the size of p (the factor found) of n

We can assume that $p \leq \sqrt{n}$)

$\boxed{\text{Examples Algs}}$

(1) Trial division $O(p(\log n)^2)$

(2) Pollard's ρ-method 1980, (1975) U.P.A.

$$O(p^{1/2}(\log n)^2)$$

③ Pollard's $p-1$ method (1974)

$$O(B \log B (\log n)^2),$$

B is a smooth bound

large B makes slow but more likely produce factors.

④ Lenstra's Elliptic curve method (1987)

U.P.A.

exp. run. time

$$O\left(\exp\left(c\sqrt{\log p \log \log p}\right) \cdot (\log n)^2\right)$$

$c \simeq 2$ (const.)

$O((\log n)^2)$ cost of performing arithmetic ops on $\mathbb{Z}$. where $O(\log n)$ or $O((\log n)^2)$ bits long

Background for NFS

Observation for G.P. Algo

For factoring n → find a suitable pair (x, y) s.t.

$$x^2 \equiv y^2 \pmod{n} \text{ but } x \not\equiv \pm y \pmod{n}$$

then there is a good chance to factor n:

$$\text{Prob.}\left(\gcd(x \pm y, n) = (f_1, f_2)_{1 < f_1, f_2 < n}\right) > \frac{1}{2}$$

In practice,
the asympt. ~ faster G.P. factg algo is the NFS & r.t.

$$O\left(\exp\left(c(\log)^{1/3}(\log\lg n)^{2/3}\right)\right)$$

—— o ——

Algebraic Number

$\alpha \in \mathbb{C}$ alg. no.

if $f(\alpha) = 0$, $f(x) = a_0 x^k + a_1 x^{k-1} + \dots + a_k$

$a_0, a_1, \dots, a_k \in \mathbb{Q}$ & $a_0 \neq 0$

— if $f(x)$ is irr. $|\ \mathbb{Q}$ & $a_0 \neq 0$
$k \to$ deg.

$\boxed{\text{Example}}$ all rational no.s are alg. no. of deg 1.

①

② $\sqrt{2}$ of deg 2 $\because f(\sqrt{2}) = (\sqrt{2})^2 - 2 = 0$

$f(x) = x^2 - 2$

any $\alpha \in \mathbb{C}$ which is not alg. is called transcendental

π & e.

$\boxed{\text{Algebraic integer}}$ A.I.

$\beta \in \mathbb{C}$ alg. integer if

$f(\beta) = 0$, $f(x) = x^k + b_1 x^{k-1} + \dots + b_k$

monic poly.

$b_0, b_1, \dots, b_k \in \mathbb{Z}$

Remark:

① quadratic integer A.I. satis quadratic Eqn

② cubic ″

Ex: ① Ordinary (rational) integers

alg. integers of deg 1 i.e. they satisfy $x - a = 0$ for $a \in \mathbb{Z}$

② $(2)^{1/3}$ & $(3)^{1/5}$ as
$x^3 - 2 = 0$ $x^5 - 3 = 0$

③ $(-1 + \sqrt{-3})/2$ as $x^2 + x + 1 = 0$

④ Gaussian integers $a + b\sqrt{-1}$, $a, b \in \mathbb{Z}$

Every A.I. is an alg. no. but revers is not true.

$\boxed{\text{Prop.}}$ A rational no. $r \in \mathbb{Q}$ is an alg. integr iff $r \in \mathbb{Z}$

□ If $r \in \mathbb{Z}$ then r is a root of $x - r = 0$

($\Leftarrow$) $\Rightarrow$ r is an alg. int. (A.I.)

($\Rightarrow$) Suppose that $r \in \mathbb{Q}$ & r is an A.I.

$\Rightarrow r = c/d$ is a root of $\qquad c, d \in \mathbb{Z}$

$$x^k + b_1 x^{k-1} + \cdots + b_k = 0, \quad b_i \in \mathbb{Z}$$

we may assum. $\gcd(c, d) = 1$ Put $r = \frac{c}{d}$

$$c^k + b_1 c^{k-1} d + b_2 c^{k-2} d^2 + \cdots + b_k d^k = 0$$

$\Rightarrow d \mid c^k$ & $d \mid c$ ($\because \gcd(c, d) = 1$)

again $\because \gcd(c, d) = 1 \Rightarrow d = \pm 1 \Rightarrow r = \frac{c}{d} \in \mathbb{Z}$ ▨

e.g. $\frac{2}{5}$ is an alg. no. but not A.I.

$\boxed{\text{Remark}}$ The elements of $\mathbb{Z}$ (rational int.) are the only rational no.s that are A.I.

$\sqrt{2}$ is alg. int. but not a rational int.

Th. The set of alg. no's form a field & the set of alg. $\mathbb{Z}$ forms a ring.

$\boxed{\text{Lemma}}$ $f(x)$ irr. poly of deg d over $\mathbb{Z}$ & $m \in \mathbb{Z}$ s.t. $f(m) \equiv 0 \pmod{n}$.

Let α be a complex root of $f(x)$ &

$\mathbb{Z}[\alpha]$ = set of all polys in α with integers coff. Then $\exists$ a $!$ mapping

$$\phi : \mathbb{Z}[\alpha] \longmapsto \mathbb{Z}_n \text{ satisfying}$$

1. $\phi(ab) = \phi(a)\phi(b), \ \forall a, b \in \mathbb{Z}[\alpha]$
2. $\phi(a+b) = \phi(a) + \phi(b), \ \forall a, b \in \mathbb{Z}[\alpha]$
3. $\phi(za) = z\,\phi(a), \ \forall a \in \mathbb{Z}[\alpha], z \in \mathbb{Z}$
4. $\phi(1) = 1$
5. $\phi(\alpha) = m \pmod{n}$