24th May

Tuesday, May 17, 2022 7:57 PM

Primality and Factoring

p – odd prime

q – any number

$$\left(\frac{q}{p}\right) = (-1)^u$$

$$q = px_1 + r_1$$
$$2q = px_2 + r_2$$
$$\vdots$$
$$\left(\frac{p-1}{2}\right)q = px_{\left(\frac{p-1}{2}\right)} + r_{\left(\frac{p-1}{2}\right)}$$

$$m = x_1 + \cdots + x_{\left(\frac{p-1}{2}\right)}$$

$m, u, p, q \pmod 2$

$$q\left[\underbrace{1 + 2 + \cdots + \frac{p-1}{2}}\right] = p\left(\underbrace{\sum x_i}_{m}\right) + \left(\sum r_i\right)$$

$$\frac{q(p^2-1)}{8} = pm + \left(\sum r_i\right)$$

$> \frac{p}{2}$ – u no. of r_i's

$$\frac{q(p^2-1)}{8} \equiv pm + \underbrace{(r_{i_1} + \cdots)}_{<p/2} + \underbrace{(r_{j_1} + \cdots + r_{j_u})}_{>p/2} \pmod 2$$

$$r_{j_1} + 2(p - r_{j_1}) = p + \underbrace{(p - r_{j_1})}_{<p/2}$$

$$\frac{q(p^2-1)}{8} \equiv pm + pu + \underbrace{(r_{i_1} + \cdots)}_{<p/2} + \underbrace{((p - r_{j_1}) + \cdots)}_{<p/2}$$

$$\underbrace{1 + 2 + \cdots + \frac{p-1}{2}}_{\frac{p^2-1}{8}}$$

$$\Rightarrow \left(\frac{p^2-1}{8}\right)(q-1) \equiv pm + pu \pmod 2$$

div by 8 · div by 2

$$- \qquad \pmod 2$$

$$\frac{(p+1)(p-1)(q-1)}{8} \equiv m + u \pmod 2$$

(div by 8 · div by 2)

$(q - \text{odd})$

$4k+1$	$4k+3$
$(p+1)(p-1)$	$(p+1)(p-1)$
$(4k+2)(4k)$	$(4k+4)(4k+2)$
8	8

$$\Rightarrow \quad 0 \equiv m + u \pmod 2$$

$$2u \equiv m + u \pmod 2$$

$$\Rightarrow \quad \boxed{u \equiv m \pmod 2}$$

Thm: Quad. reciprocity Theorem: p, q – odd primes $(p \neq q)$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

$p = 4k-1$, $q = 4l-1$

$\left(\frac{p}{q}\right) = 1$, $\left(\frac{q}{p}\right) = ? = -1$

$\left(\frac{p-1}{2}\right) = 2k-1 = \text{odd}$

$\left(\frac{q-1}{2}\right) = \text{odd}$

$$\left(\frac{p}{q}\right) = (-1)^u \qquad \left(\frac{q}{p}\right) = (-1)^v$$

$\{p, 2p, \dots, \left(\frac{q-1}{2}\right)p\}$ $(\bmod q)$ $> \frac{q}{2} \rightarrow \boxed{u}$

$\{q, 2q, \dots, \left(\frac{p-1}{2}\right)q\}$ $(\bmod p)$ $> \frac{p}{2} \rightarrow \boxed{v}$

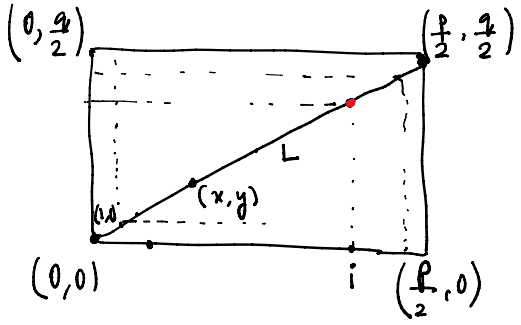
$$(\quad)^{u+v} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$(-1)^{u+v} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$u+v \equiv \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \pmod 2$$

$$m+n \equiv \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \pmod 2$$

$$\begin{cases} m = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \left(\frac{q-1}{2}\right)\frac{p}{q} \right\rfloor \\ n = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \left(\frac{p-1}{2}\right)\frac{q}{p} \right\rfloor \end{cases}$$



$$\frac{x}{p/2} = \frac{y}{q/2} \Rightarrow qx = py$$

$$0 < x \le \frac{p-1}{2}$$

$$0 < y \le \frac{q-1}{2}$$

no integer points on L.

$$y = \frac{qi}{p} \qquad \lfloor 7 \cdot \tfrac{3}{5} \rfloor$$

1, 2, ... 7

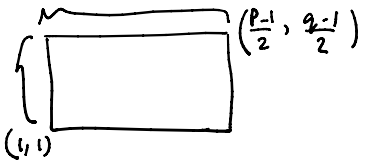
pts. below L:

$x = i$: $y \le \frac{qi}{p} \Rightarrow$ no. of pts $= \left\lfloor \frac{qi}{p} \right\rfloor$

$$\text{total} = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \left(\frac{p-1}{2}\right)\frac{q}{p} \right\rfloor = n$$

pts above L:

total $= m$



$$\left(\frac{p-1}{2} - x + x\right)\left(\frac{q-1}{2} - x + x\right) = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = m+n$$

$$u+v \equiv m+n = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \pmod 2$$

(-1) (-1)

PRIMALITY TESTING

* Given a number $n \in \mathbb{N}$. Is it prime?

count = 0 & 2

$n = 143$ ✓

1 (2) 3 4 5 6 7 8 9 10 [11] 12 13 14

✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✓ ✗ ✓ ✗ ....

$[2 \ldots n-1]$ → Time complexity = ??

* Time Complexity of Algorithms??

$A = [a_1, a_2, \ldots, a_n]$

Sum of all elements = ?

```
sum=0
For (i=1 ; i≤n ; i++))
    sum += a[i]
return sum
```

Total time = $c_2 n$

Time complexity = $O(n)$

Assumptions :-
- → Arithmetic operations takes constant time
- → Assignment taks constant time

---

a=0 → c_1 time
b=2
c=2+0 → c_2 time
d=0 → c_1 time
e=d+c → c_2 time

* Algo.1 :- Input $n \in \mathbb{N}$

1. If $\exists\ 2 \le k \le n-1$ s.t. $n \% k == 0$
   then OUTPUT "composite"
   else OUTPUT "Prime!!"

→ At max this may take $n-1$ steps

Time = $\lambda(n-1) = O(n)$

Q. Can we do better??

Observation :- (Ex) A number $2 < n$ is prime iff $\forall\ 2 \le k \le \lceil \sqrt{n} \rceil$ ✓ $k \nmid n$.

→ $\{2, 3, 4, \ldots, 34\}$

$n = 35$ ✗ $[\{2, 3, 4, 5, 6\}]$

✗ ✗ ✗ ✓

Time Complexity = $O(\sqrt{n})$ ←

$n \ldots < MAX$

Q. Given $2 \le n_1, n_2, \ldots, n_K \le MAX$

Time $= O(\sqrt{n_1} + \sqrt{n_2} + \cdots + \sqrt{n_K})$

$= O(K\sqrt{MAX})$ → $n \log n$

MAX = 20 → TC = $O(n \log n)$

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~

$2 \le 10^4 \le 20$ $\quad O(10^4 \sqrt{20})$

$O(20 \log 20 + 10^4) \approx O(10^4)$

1, 2, 3, ..., n

Steps = $\frac{n}{2} + \frac{n}{3} + \frac{n}{5} + \cdots + \frac{n}{p}$ where p is largest prime $\le n$

$= n\left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p}\right)$

[Fact:- $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} \approx \log\log p_n$; $p_1 = 2$, $p_2 = 3$, $p_n = n^{th}$ prime]

$\le n\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right)$ → $\log n$

$\le n \log n$

[$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ | $\lim_{n\to\infty} |H_n - \log n| \to \gamma$, $\gamma = 0.577$]

$H_n \approx \log n$

1, 1, 1, 1, 1, 1, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, $\frac{1}{5}$, $\frac{1}{6}$, $\frac{1}{7}$, $\frac{1}{8}$, $\frac{1}{9}$, $\frac{1}{10}$, $\frac{1}{11}$, $\frac{1}{12}$, $\frac{1}{13}$, $\frac{1}{14}$, $\frac{1}{15}$, $\frac{1}{16}$, $\frac{1}{17}$, $\frac{1}{18}$, $\frac{1}{19}$, $\frac{1}{20}$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16} = 2^4$$

$$\leq 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} \cdots + \frac{1}{8}$$

$$\leq 1 + 1 + 1 + 1 = 4 \qquad 2^{\textcircled{4}} \leq \textcircled{4}$$

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

$$\leq 1 + \frac{1}{2} + \cdots + \frac{1}{n} + \cdots \frac{1}{2^k}$$

$$\leq k \propto \log_2 n$$

$n \leq 2^k \leq 2n$

$\log n \leq k \leq \log 2 + \log n$

$\rightarrow k \approx \log n$

$O(q\sqrt{max})$

If we had q such queries the total time $= O(Max \log Max + q)$ ✓

FACTORING

★ Given n, factorize n.

Suggestion 1 → $n \log n + \frac{n}{\log n} \times \log n = n \log n$

$n = 177973 = 17 \cdot 19^2 \cdot 29$

$n \rightarrow \frac{n}{17}$

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

(17,1)
(19,2)
(29,1)

$n = 17 \cdot 19^2 \cdot 29$

$\rightarrow 19^2 \cdot 29 \rightarrow 19 \cdot 29 \rightarrow 29 \rightarrow \boxed{1}$

TC → $n \cdot \log n$

* Given k numbers $2 \le a_1, \ldots, a_k \le n$, factorize all of them

→ LINEAR SIEVE ←

$T = O(n + k \log n)$ ($\log n$: small)

$(kn \log n)$ → earlier

↳ (i) It gives a list of all primes $\le n$

(ii) It gives the smallest prime factor $\forall\ 2 \le k \le n$

$lp[i]$ = smallest prime factor of i

(iii) It takes $O(n)$ time to do so.

```
void sieve()
{
    for (Long Long i=2; i <= N; ++i) {
        if (lp[i] == 0) {
            lp[i] = i;
            pr.push_back(i);
        }
        for (Long Long j=0; j < (Long Long)pr.size() && pr[j] <= lp[i] && i*pr[j] <= N; ++j) {
            lp[i * pr[j]] = pr[j];
        }
    }
}
```

n = 10

pr = | 2 | 3 | 5 | 7 | | | | |

$lp[i \cdot p_k] = p_k$ (p_k)

lp =

1	2	3	4	5	6	7	8	9	10
0	2	3	2	5	2	7	2	3	2

TC = O(n)

* 20 $(2,2^2)$ $(2,2)$, $(5,1)$

10 $(5,1)$ $2^2 \times 5^1$

5

1

* If we have access to lp[], then factors of n can be found in O(log n).