Class 07

Thursday, September 23, 2021 9:15 PM

```
for(i=1; i≤n; i++)
  for(j=i; j≤n; j+=i)
    → divSum[j] += i;
    → divCount[j]++;
    → divList[j].push_back(i);
```

— o —

Prime factorization of number

$$12 = 2\times 2\times 3 = 2^{2}\times 3^{1}$$

#divisors → $(2+1)(1+1)$
$= 3\times 2$
$= 6$

$$18 = 2\times 3^{2} = 2^{1}\times 3^{2}$$

sum of divisors → $\dfrac{2^{2}-1}{2-1}\times\dfrac{3^{3}-1}{2}$
$= 3\times 13$

$$N = p_1^{\alpha_1}\times p_2^{\alpha_2}\times \cdots\cdots \times p_k^{\alpha_k}$$

→ #divisors → $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$
→ $\prod_{i=1}^{k}(\alpha_i+1)$

→ sum of divisors → $\prod_{i=1}^{k}\left(\dfrac{p_i^{\alpha_i+1}-1}{p_i-1}\right)$

$$N = 2^{3}\times 3^{2}\times 7^{4}$$

$$\left(\frac{2^{4}-1}{2-1}\right)\times\left(\frac{3^{3}-1}{3-1}\right)\times\left(\frac{7^{5}-1}{7-1}\right)$$

$= 15\times 13\times 2801$

$=$

— o —

$16 = 2^{4}$ → $1, 2, 4, 8, 16$ → $2^{0}, 2^{1}, 2^{2}, 2^{3}, 2^{4}$

$N = p^{k}$

$12 = 2^2 \times 3^1 \times 5^2 \rightarrow$

	2^0	2^1	2^2
3^0	1	2	4
3^1	3	6	12

$\rightarrow (2+1)$

$(1+1)$

$(2+1)\ (1+1)$

$\rightarrow k+1$

$T_{mx} = 10^3$

$N_{mx} = 10^{12}$

— ∘ —

$$O(\sqrt{N}) \approx 10^6 \times 10^3 \approx 10^9 > 10^8$$

$$N = (10^6 + k_1)^2 > N_{max}$$

$k_1, k_2 > 0$

$N \leq 10^{12}$

$$N = 10^9 + 7$$

$$\frac{N}{\ln N} \rightarrow \frac{\sqrt{N}}{\ln \sqrt{N}}$$

p_0

$\sqrt{N}$

— ∘ —

$$(\log N)^2 \approx 3600$$

99.9999999%

Miller-Rabin → Large Number Primality Testing

Pollard-Rho → Large Number Divisor Finding

— o —

Modular Arithmetic

1) $(A+B)\%M = ((A\%M)+(B\%M))\%M$

2) $(A-B)\%M = ((A\%M)-(B\%M)+M)\%M$

3) $(A\times B)\%M = ((A\%M)\times(B\%M))\%M$

$(12+17)\%5 \rightarrow 4$

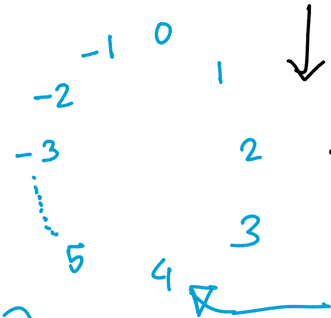
$(2+2)\%5 \rightarrow 4$

$(12\times 17)\%5 \rightarrow 4$

$(2\times 2)\%5 \rightarrow 4$

$(17-13)\%5 \rightarrow 4$

$(\underbrace{2-3}+5)\%5 \rightarrow 4$



$\downarrow a-b\uparrow$

$\cancel{0-4}$

$-4+5$

Modulo value $\rightarrow (4+5k)\%5 = 4$

$-6, -1, 4, 9, 14, 19, 24, \ldots\ldots$

— o —

Next Topic

Fermat's Little Theorem

Modulo inverse

BigMOD