QUICK COMPUTATION OF THE PARITY OF $\prod(x)$

By H. LIFCHITZ

March 1998 (corrected on October 2001)

Let $\prod(x)$ = Number of prime numbers below or equal to x.

$\lfloor x \rfloor$=integer part of x, and $\Omega(x)$ the number of prime divisors of x (with repetition).

$\Omega(x)$ is additive, $\Omega(1) = \Omega(0) = 0$, $\Omega(p) = 1$ and $\Omega(x.y) = \Omega(x) + \Omega(y)$

$$\boxed{\Omega(x!) = \sum_{P_i \le x} \left\lfloor \frac{x}{P_i} \right\rfloor + \sum_{P_i \le x^{1/2}} \left\lfloor \frac{x}{{P_i}^2} \right\rfloor + \sum_{P_i \le x^{1/3}} \left\lfloor \frac{x}{{P_i}^3} \right\rfloor + \cdots} \qquad (1)$$

Indeed $x! = 2^{\lfloor \frac{x}{2} \rfloor + \lfloor \frac{x}{2^2} \rfloor + \cdots} .3^{\lfloor \frac{x}{3} \rfloor + \lfloor \frac{x}{3^2} \rfloor + \cdots} .5^{\lfloor \frac{x}{5} \rfloor + \lfloor \frac{x}{5^2} \rfloor + \cdots} \cdots$, therefore

$$\Omega(x!) = \left\lfloor \tfrac{x}{2} \right\rfloor + \left\lfloor \tfrac{x}{2^2} \right\rfloor + \left\lfloor \tfrac{x}{2^3} \right\rfloor + \cdots$$

$$+ \left\lfloor \tfrac{x}{3} \right\rfloor + \left\lfloor \tfrac{x}{3^2} \right\rfloor + \left\lfloor \tfrac{x}{3^3} \right\rfloor + \cdots$$

$$\vdots \qquad \vdots \qquad \vdots$$

Summing vertically we obtain (1)

$$\boxed{\sum_{P_i \le x^{1/a}} \left\lfloor \frac{x}{{P_i}^a} \right\rfloor = \sum_{i=1}^{i=\lfloor \frac{x}{2^a} \rfloor} \prod \left[\left(\frac{x}{i} \right)^{1/a} \right]} \qquad (2)$$

Indeed $\left\lfloor \frac{x}{{P_i}^a} \right\rfloor = 1$ when $1 \le \frac{x}{{P_i}^a} < 2$ or $\frac{x}{2} < {P_i}^a \le x$ or $\left(\frac{x}{2}\right)^{1/a} < P_i \le x^{1/a}$

Therefore $\displaystyle\sum_{P_i \le x^{1/a}} \left|\frac{x}{{P_i}^a}\right| = \sum_{P_i \le \left(\frac{x}{2}\right)^{1/a}} \left|\frac{x}{{P_i}^a}\right| + \prod\left[x^{1/a}\right] - \prod\left[\left(\frac{x}{2}\right)^{1/a}\right]$

afterwards $\displaystyle\sum_{P_i \le x^{1/a}} \left|\frac{x}{{P_i}^a}\right| = \sum_{P_i \le \left(\frac{x}{3}\right)^{1/a}} \left|\frac{x}{{P_i}^a}\right| + \prod\left[x^{1/a}\right] - \prod\left[\left(\frac{x}{2}\right)^{1/a}\right] - 2\prod\left[\left(\frac{x}{3}\right)^{1/a}\right]$

and comes (2) continuing the process.

Let $\boxed{\displaystyle\Psi_\Omega(x) = \sum_{i=1}^{i=|log_2 x|} \prod\left(x^{1/i}\right)}$ (3)

By moebius inversion we have $\boxed{\displaystyle\prod(x) = \sum_{i=1}^{i=|log_2 x|} \mu(i)\Psi_\Omega\left(x^{1/i}\right)}$ (4)

Then we have $\boxed{\displaystyle\sum_{i \le x}\Psi_\Omega\left(\frac{x}{i}\right) = \Omega(x!)}$ (5)

because $\displaystyle\sum_{i \le x}\Psi_\Omega\left(\frac{x}{i}\right) = \sum_{P_i \le x}\left|\frac{x}{P_i}\right| + \sum_{P_i \le \left|x^{1/2}\right|}\left|\frac{x}{{P_i}^2}\right| + \sum_{P_i \le \left|x^{1/3}\right|}\left|\frac{x}{{P_i}^3}\right| + \cdots$

Inverting (5) comes $\boxed{\displaystyle\Psi_\Omega(x) = \sum_{i \le x}\mu(i)\Omega\left[\left(\frac{x}{i}\right)!\right]}$ (6)

Expanding the right part of (6) we find :

$$\Psi_\Omega(x) = \sum_{P_i \le x}\left|\frac{x}{P_i}\right| - 2*\sum_{P_i < P_j \le x}\left|\frac{x}{P_i.P_j}\right| + 3*\sum_{P_i<P_j<P_k \le x}\left|\frac{x}{P_i.P_j.P_k}\right| - 4*\sum_{P_i<P_j<P_k<P_l \le x}\left|\frac{x}{P_i.P_j.P_k.P_l}\right| + \cdots$$

Let $\displaystyle A_1(x) = \sum_{P_i \le x}\left|\frac{x}{P_i}\right|, A_2(x) = \sum_{P_i<P_j \le x}\left|\frac{x}{P_i.P_j}\right|, A_3(x) = \sum_{P_i<P_j<P_k \le x}\left|\frac{x}{P_i.P_j.P_k}\right|, etc\cdots$

Then $\boxed{\Psi_\Omega(x) = A_1(x) - 2.A_2(x) + 3.A_3(x) - 4.A_4(x) + \cdots}$ (7)

But $\displaystyle\sum_{i \le x}\mu(i)\left|\frac{x}{i}\right| = 1$

Also let $\boxed{x - 1 = A_1(x) - A_2(x) + A_3(x) - A_4(x) + \cdots}$ (8)

(7)-(8) result in $\boxed{\Psi_\Omega(x) = x - 1 - A_2(x) + 2.A_3(x) - 3.A_4(x) + 4.A_5(x) - \cdots}$ (9)

We note that $\Psi_\Omega(x) = x - 1$ for $1 < x < 6$ and $\Psi_\Omega(0) = 0$

So we have $\boxed{\Psi_\Omega(x) \equiv x - 1 - A_2(x) - A_4(x) - A_6(x) - \cdots \pmod 2}$ (10)

But $$\boxed{\sum_{i\le x} Q\left(\frac{x}{i}\right) = 2(A_2(x)+A_4(x)+A_6(x)+\cdots)+2x-1} \qquad (11)$$

with $Q(x)$ number of "squarefree" $\le x$

Indeed let $\prod_k(x)$ = number of "squarefree" $\le x$ having k prime factors, we also have :

$$A_1(x) = \sum_{i\le\left|\frac{x}{2}\right|} \prod\left(\frac{x}{i}\right), \quad A_2(x) = \sum_{i\le\left|\frac{x}{6}\right|} \prod{}_2\left(\frac{x}{i}\right), \quad A_3(x) = \sum_{i\le\left|\frac{x}{30}\right|} \prod{}_3\left(\frac{x}{i}\right), etc\cdots$$

and $A_1(x)+A_2(x)+A_3(x)+A_4(x)+\cdots = \sum_{i\le\left|\frac{x}{2}\right|} \prod\left(\frac{x}{i}\right) + \sum_{i\le\left|\frac{x}{6}\right|} \prod_2\left(\frac{x}{i}\right) + \sum_{i\le\left|\frac{x}{30}\right|} \prod_3\left(\frac{x}{i}\right) + \cdots$

But $Q(x) = 1+\prod(x)+\prod_2(x)+\prod_3(x)+\prod_4(x)+\cdots$

So $$\boxed{A_1(x)+A_2(x)+A_3(x)+A_4(x)+\cdots = \sum_{i\le x} Q\left(\frac{x}{i}\right) - x} \qquad (12)$$

Let $SQ(x) = \sum_{i\le x} Q\left(\frac{x}{i}\right)$

(8) and (12) result in $2(A_2(x)+A_4(x)+A_6(x)+A_8(x)+\cdots) = SQ(x)-2x+1$, which proves (11)

and also $$\boxed{SQ(x) = \sum_{i\le x} Q\left(\frac{x}{i}\right) \equiv 1 \pmod 2 \quad \forall x} \qquad (13)$$

(10) et (11) result in $$\boxed{\Psi_\Omega(x) \equiv \tfrac{SQ(x)-1}{2} \pmod 2} \qquad (14)$$

Let $F1(x) = \sum_{i\le x} \left|\frac{x}{i}\right|$, it is easy to show that $F1(x) = 2\sum_{i=1}^{i=|\sqrt{x}|} \left|\frac{x}{i}\right| - |\sqrt{x}|^2$

Let $\boxed{F1r(x) = \sum_{i\le|\sqrt{x}|} \left|\frac{x}{i}\right|}$, so we have $F1(x) = 2.F1r(x) - |\sqrt{x}|^2$ and $\boxed{F1(x) \equiv |\sqrt{x}| \pmod 2}$ (15)

But $\boxed{F1(x) = \sum_{i\le|\sqrt{x}|} SQ\left(\frac{x}{i^2}\right)}$ (16) and by moebius inversion $\boxed{SQ(x) = \sum_{i\le|\sqrt{x}|} \mu(i).F1\left(\frac{x}{i^2}\right)}$ (17)

So $SQ(x) = \sum_{i\le|\sqrt{x}|} \mu(i)\left[2.F1r\left(\frac{x}{i^2}\right) - \left|\sqrt{\frac{x}{i^2}}\right|^2\right] = 2\sum_{i\le|\sqrt{x}|} \mu(i).F1r\left(\frac{x}{i^2}\right) - \sum_{i\le|\sqrt{x}|} \mu(i).\left|\frac{\sqrt{x}}{i}\right|^2$

Let $$\boxed{SQ_1(x) = \tfrac{SQ(x)-1}{2} = \sum_{i\le|\sqrt{x}|} \mu(i).F1r\left(\frac{x}{i^2}\right) - \left(\frac{\sum_{i\le|\sqrt{x}|} \mu(i)\left|\frac{\sqrt{x}}{i}\right|^2 + 1}{2}\right)} \qquad (18)$$

Let $SR(x) = \sum_{i \leq \lfloor \sqrt{x} \rfloor} \mu(i) \left\lfloor \frac{\sqrt{x}}{i} \right\rfloor^2$

$\left\lfloor \frac{\sqrt{x}}{i} \right\rfloor = 1$ for $\frac{\sqrt{x}}{2} < i \leq \sqrt{x}$, so $SR(x) = \sum_{i \leq \lfloor \frac{\sqrt{x}}{2} \rfloor} \mu(i) \left\lfloor \frac{\sqrt{x}}{i} \right\rfloor^2 + \sum_{i=\lfloor \frac{\sqrt{x}}{2} \rfloor+1}^{i=\lfloor \sqrt{x} \rfloor} \mu(i)$

$\left\lfloor \frac{\sqrt{x}}{i} \right\rfloor = 2$ for $\frac{\sqrt{x}}{3} < i \leq \frac{\sqrt{x}}{2}$, so $SR(x) = \sum_{i \leq \lfloor \frac{\sqrt{x}}{3} \rfloor} \mu(i) \left\lfloor \frac{\sqrt{x}}{i} \right\rfloor^2 + 4 \sum_{i=\lfloor \frac{\sqrt{x}}{3} \rfloor+1}^{i=\lfloor \frac{\sqrt{x}}{2} \rfloor} \mu(i) + \sum_{i=\lfloor \frac{\sqrt{x}}{2} \rfloor+1}^{i=\lfloor \sqrt{x} \rfloor} \mu(i)$

Continuing the process comes $SR(x) = \sum_{i=1}^{i=\lfloor \sqrt{x} \rfloor} i^2 \sum_{j=\lfloor \frac{\sqrt{x}}{i+1} \rfloor+1}^{j=\lfloor \frac{\sqrt{x}}{i} \rfloor} \mu(j)$

Seeing that $x^2 \equiv 0 \pmod 4$ for even x and $x^2 \equiv 1 \pmod 4$ for odd x

we have $SR(x) \equiv \sum_{\text{i odd} \leq \lfloor \sqrt{x} \rfloor} \sum_{j=\lfloor \frac{\sqrt{x}}{i+1} \rfloor+1}^{j=\lfloor \frac{\sqrt{x}}{i} \rfloor} \mu(j) \pmod 4$

But $\sum_{i=a+1}^{i=b} \mu(i) = M(b) - M(a)$ with $M(x)$ Moebius summatory function

So $SR(x) \equiv M(\sqrt{x}) - M\left(\frac{\sqrt{x}}{2}\right) + M\left(\frac{\sqrt{x}}{3}\right) - M\left(\frac{\sqrt{x}}{4}\right) + \cdots \pmod 4$

But $M(x) - M\left(\frac{x}{2}\right) + M\left(\frac{x}{3}\right) - M\left(\frac{x}{4}\right) + \cdots = -1$ property of $M(x)$ for $x \geq 2$

So $SR(x) = \sum_{i \leq \sqrt{x}} \mu(i) \left\lfloor \frac{\sqrt{x}}{i} \right\rfloor^2 \equiv -1 \pmod 4$ for $x \geq 4$

And (18) results in $$\boxed{SQ_1(x) \equiv \sum_{i \leq \lfloor \sqrt{x} \rfloor} \mu(i) F1r\left(\frac{x}{i^2}\right) \pmod 2} \qquad (19)$$

So $$\boxed{\Psi_\Omega(x) \equiv SQ_1(x) \pmod 2} \qquad (20)$$

And finally with (4) $$\boxed{\boxed{\prod(x) \equiv \sum_{i=1}^{i=\lfloor log_2 x \rfloor} \mu(i) SQ_1(x^{1/i}) \pmod 2}} \qquad (21)$$

This expression allows to compute the parity of $\prod(x)$ with a complexity in $O\,(x^{1/2}.logx)$ and with

a storage space in $O(1)$.