Lehman's Factoring Method

Our object is to present the factoring algorithm of R. Sherman Lehman (*Facoring large integers*, Math. Comp. **28** (1974), 637–646) in a simplified and transparent manner.

Theorem 1. *Suppose that $n = ab$ where a and b are integers such that*

$$n^{1/3} < a \le n^{1/2} \le b < n^{2/3}\,.$$

Then there exist integers k, x, and y such that

$$4kn = x^2 - y^2, \tag{1}$$

$$1 \le k \le n^{1/3} + 1, \tag{2}$$

$$(4kn)^{1/2} \le x \le (4kn)^{1/2} + \frac{n^{1/6}}{4k^{1/2}}\,, \tag{3}$$

$$0 \le y \le n^{1/3}\,. \tag{4}$$

Proof. We recall that Dirichlet's theorem asserts that if S is a real number, $S \ge 1$, and if θ is a real number, then there exists an integer s, $1 \le s \le S$, such that $\|\theta s\| \le 1/S$. Here $\|u\| = \min_{n\in\mathbb{Z}} |u - n|$ is the distance from u to the nearest integer. (This is the natural metric on the circle group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$.) Take $\theta = b/a$, $S = a/n^{1/3}$. Thus there are integers r and s such that

$$\left|\frac{bs}{a} - r\right| \le \frac{n^{1/3}}{a}\,, \tag{5}$$

with $1 \le s \le a/n^{1/3}$. On multiplying by a, it follows that

$$|bs - ar| \le n^{1/3}\,. \tag{6}$$

From (5) we also see that $r > 0$, since $bs/a \ge 1$ and $n^{1/3}/a < 1$. Also from (5) we see that

$$r \le \frac{bs}{a} + \frac{n^{1/3}}{a}\,.$$

Since $s \le a/n^{1/3}$, it follows that

$$1 \le rs \le \frac{bs^2}{a} + \frac{n^{1/3}s}{a} \le n^{1/3} + 1\,.$$

We take $k = rs$, and note that (2) is satisfied. Set $x = ar + bs$, $y = |ar - bs|$. Then

$$x^2 - y^2 = (ar + bs)^2 - (ar - bs)^2 = 4arbs = 4kn\,.$$

Thus (1) is satisfied. By (6) we see that (4) is also satisfied. It remains to show that (3) holds. To this end we note that $x^2 = 4kn + y^2$. Hence

$$(4kn)^{1/2} \le x \le (4kn + y^2)^{1/2} \le \big(4kn + n^{2/3}\big)^{1/2} = (4kn)^{1/2}\Big(1 + \frac{1}{4kn^{1/3}}\Big)^{1/2}.$$

The inequality $(1+u)^{1/2} \le 1 + u/2$ holds for all real $u \ge -1$. Hence the above is

$$\le (4kn)^{1/2}\Big(1 + \frac{1}{8kn^{1/3}}\Big) = (4kn)^{1/2} + \frac{n^{1/6}}{4k^{1/2}}\,.$$

Thus we have (3), and the proof is complete.

As a partial converse to Theorem 1, we prove

Theorem 2. *Suppose that $n \ge 8$, and that there exist integers k, x, and y such that* (1)–(4) *hold. Then $(n, x+y)$ and $(n, x-y)$ are proper divisors of n.*

Proof. From (1) we see that $n|(x+y)(x-y)$. Thus if $(n, x+y) = 1$, then $n|(x-y)$, and if $(n, x-y) = 1$, then $n|(x+y)$. Hence it suffices to show that $n \nmid (x+y)$ and that $n \nmid (x-y)$. We achieve this by showing that $0 < x - y \le x + y < n$. From (2)–(4) we see that

$$y \le n^{1/3} < (4n)^{1/2} \le (4kn) \le x\,.$$

Hence $x - y > 0$. On the other hand, from (3) and (4) we see that

$$x + y \le (4kn)^{1/2} + \frac{n^{1/6}}{4k^{1/2}} + n^{1/3}\,. \tag{7}$$

Put

$$f(u) = (4un)^{1/2} + \frac{n^{1/6}}{4u^{1/2}} + n^{1/3}.$$

It is easy to verify that f is increasing. Set $K = [n^{1/3} + 1]$. From (7) we deduce that

$$x + y \le 2K^{1/2}n^{1/2} + \frac{n^{1/6}}{4K^{1/2}} + n^{1/3} \le 2K^{1/2}n^{1/2} + n^{1/3} + \frac{1}{4}$$

since $K \ge n^{1/3}$. In the opposite direction we find that

$$K^{1/2} \le \big(n^{1/3} + 1\big)^{1/2} = n^{1/6}\Big(1 + \frac{1}{n^{1/3}}\Big)^{1/2} \le n^{1/6}\Big(1 + \frac{1}{2n^{1/3}}\Big) = n^{1/6} + \frac{1}{2n^{1/6}}.$$

Hence $x+y \le 2n^{2/3}+2n^{1/3}+1$. Put $g(u)=u^3-2u^2-2u-1$. Since $g(u)=(u-3)(u^2+u+1)+2$, it is clear that $g(u)>0$ for $u \ge 3$. Hence $2n^{2/3}+2n^{1/3}+1<n$, and the proof is complete.

Suppose we know that n has no factor $\le n^{1/3}$. Then n is either prime, or the product of two primes. If the system (1)–(4) has no solution, then n is prime. If it has a solution, then the prime factors of n are the numbers $(n, x \pm y)$. To search for a solution, put $K=[n^{1/3}+1]$. For each x in the interval (3) we test to see whether x^2-4kn is a perfect square, say by the square-detecting algorithm described on pp. 38–41 of H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag (Berlin). The number of tests is

$$\ll \sum_{k=1}^{K}\left(\frac{n^{1/6}}{k^{1/2}}+1\right) \ll n^{1/6}K^{1/2}+K \ll n^{1/3}\,.$$