TUTORIAL 9

1 Modular roots and factoring, again

Last week, we saw Tonelli-Shanks algorithm to compute square roots modulo an odd prime p in $O(\log^3 p)$. The first step of this exercise is to design an algorithm to compute square roots modulo p^v, for some $v \geq 2$ and odd prime p.

1. Let $x \in (\mathbb{Z}/p^v\mathbb{Z})^\times$. Show that $x^2 \equiv 1\ [p^v]$ if and only if $x \equiv \pm 1\ [p^v]$. Let φ be the Euler totient function. Deduce a generalization of Euler's criterion:

$$x^{\varphi(p^v)/2} \equiv \begin{cases} 1 \text{ if } x \text{ is a square } \bmod p^2, \\ -1 \text{ if } x \text{ is not a square } \bmod p^2. \end{cases}$$

2. Show that an integer x coprime to p is a square modulo p if and only if it is a square modulo p^v.

   We will now use a Hensel-like strategy: assume we know $y \in (\mathbb{Z}/p^{v-1}\mathbb{Z})^\times$ a square root of x modulo p^{v-1}.

3. If z is a square root of x modulo p^v, show that $z \equiv \pm y\ [p^{v-1}]$.

4. We keep assuming z is a square root of x modulo p^v. Show that there is an integer k such that $x - y^2 \equiv \pm 2ykp^{v-1}\ [p^v]$. Then use that $2y \in (\mathbb{Z}/p\mathbb{Z})^\times$ and the previous question to give an expression for z.

5. Deduce an algorithm to compute square roots modulo p^v and give its complexity.

   The second step is to show that factoring an integer N and computing square roots modulo N are equivalent problems.

6. Write $N = p_1^{v_1} \dots p_r^{v_r}$, for some distinct primes $p_1, \dots, p_r$. Show that x is a square modulo N if and only if $x^{(p_i-1)/2} \equiv 1\ [p_i]$. Also show that a square modulo N has 2^r square roots.

7. Assume we have an algorithm A that computes square roots in $\mathbb{Z}/N\mathbb{Z}$ in time τ. Show that we can find a factor of N in expected time $O(\tau(1 - 2^{1-d}))$. Conclude on the respective difficulty of these problems.

2 McKee's factoring algorithm

An old factoring strategy is to find two different ways to represent n as a sum of two squares. Unfortunately, not any number can be represented as a sum of two squares, and, even if it can, the representation is, in general, hard to find. Nevertheless, there are algorithms that exploit this idea. In this exercise, we develop the factorization algorithm due to McKee that finds a non-trivial factor of n *provably* in time $\mathcal{O}(n^{1/2+\varepsilon})$ and *heuristically* in time $\mathcal{O}(n^{1/4} + \varepsilon)$.

Suppose $n = pq$ and $2n^{1/4} < p < q$. Let

$$b = \lceil \sqrt{n} \rceil.$$

Define

$$Q(x, y) = (x + by)^2 - ny^2.$$

The idea is to search for integers x, y s.t.

$$Q(x, y) = z^2 \tag{1}$$

for an integer z. A triple (x, y, z), as you now show, gives a non-trivial factor of n.

1. Set $r = \lfloor \sqrt{(q/p)} \rfloor$ and

$$y = 2 \cdot r, \quad x = r^2 p + q - by, \quad z = q - r^2 p.$$

   Show that

   1. (x, y, z) defined as above gives a solution to (1)
   2. $2 \leq y \leq n^{1/4}$,
   3. $0 \leq z < 2n^{1/2}$,
   4. $|x|y < 2n^{1/2}$,
   5. $\gcd(x + by - z, n)$ gives a non-trivial factor of n.

2. Using the above, give an algorithm that finds a non-trivial factor of n in time $\mathcal{O}(n^{1/2+\varepsilon})$.

3. For an heuristic version of the algorithm we would want to have many solutions to (1). Refine the results of question 1 by showing that for an integer $T > 1$:

   1. $2 < y < n^{1/4} + 2(T - 1)$,
   2. $|x|y < T^4\sqrt{n}$,
   3. $|z| < (T^2 - 1)\sqrt{n}$,
   4. there exist at least $(T - 1)$ solutions to (1) for $x > 0$.

   Our heuristic assumption states that the number of solutions to (1) is large enough so that there exist a solution triple (x, y, z) such that the following two conditions are met:

   - $\gcd(x, y, z) = 1$,
   - there exist m that divides z.

4. Show that under the above assumptions for $x > 0$ and $m^2 > 2xy$, there exist $x_0 < m^2$ and $\lambda \in \mathbb{Z}$ s.t.

$$0 < \frac{x_0}{m^2} - \frac{\lambda}{y} < \frac{1}{2y^2}.$$

   Note that λ/y can be extracted from the continued fraction expansion of x_0/m^2.

5. Knowing the above, propose a speed-up to the algorithm given in question 2. Argue informally on the achieved gain.