1 Символ Лежандра

Основные соотношения:

1. $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (mod\, p) = \begin{cases} 1, \text{ если a — квадратичный вычет,} \\ -1, \text{ иначе} \end{cases}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
4. $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, если p и q — нечетные простые.
5. $\left(\frac{a}{p}\right) = \left(\frac{a\%p}{p}\right)$

2 Алгоритм Тонелли–Шэнкса (Tonelli–Shanks)

Мы решаем уравнение $x^2 \equiv a(mod\, p)$, где p простое и решение существует
(то есть символ Лежандра $\left(\frac{a}{p}\right)$ равен 1).

1. Найти число z, которое не является квадратичным вычетом по модулю p (брать случайные, пока не попадется подходящее, вероятность этого $\frac{1}{2}$).
2. Представим $p-1$ в виде $p-1 = Q2^S$.
3. Положим $c = z^Q$, $r = a^{\frac{Q+1}{2}}$, $t = a^Q$, $M = S$.
4. Пока t не равно 1 по модулю p:
   (a) Найти наименьшее число S', такое что $t^{2^{S'}} \equiv 1(mod)$
   (b) $w = c^{2^{S-S'-1}}$
   (c) $r = rw$, $t = tw^2$, $c = w^2$, $S = S'$

r является решением уравнения $x^2 \equiv a(mod\, p)$.

3 Поднятие решения (лемма Гензеля)

Пусть a – решение уравнение $f(x) \equiv 0(mod\, p^k)$ и $f'(a) \neq 0(mod\, p)$. Тогда для любого $m \leq k$ решение уравнения $f(x) \equiv 0(mod\, p^{k+m})$ можно найти как

$$x = a - \left(\frac{f(a)}{p^k}\right)(f'(a))^{-1} p^k.$$

Здесь деление $\left(\frac{f(a)}{p^k}\right)$ понимается как обычное целочисленное деление, а все остальные операции (включая взятие обратного) производятся по модулю p^{k+m}.

Случаи, когда лемма Гензеля не работает:

1. Если $a \equiv 0(mod\, p)$. В этом случае нужно проверить, на какую степень p делится a. Если эта степень нечетная, то решения нет. Если четная, то a представляется в виде $a = p^{2t}b$, где b не делится на p. В этом случае нужно найти решение для $x \equiv b(mod\, p^k)$ и затем умножить его на p^t.

2. $p = 2$. Будем считать, что a нечетное (иначе мы попадаем в предыдущий случай). Для $mod\, 2$ решение есть всегда. Для $mod\, 4$ – только если a дает остаток 1 по модулю 4. Для $mod\, 2^k$, $k \geq 3$ корень извлекается только если $a \equiv 1(mod\, 8)$. Для того чтобы найти корень можно пользоваться следующей процедурой.

Пусть x – корень из a по модулю p^k. Если $(x^2 - a)/p^k$ четное число, то x является корнем по модулю p^{k+1}. Если же $(x^2 - a)/p^k$ нечетно, то корнем будет $x + 2^{k-1}$.