Formulas in Mathematical Cryptology

Ch 1:

CRT: $M = m_1 m_2 \cdots m_r$, $m_1, m_2, \ldots$ pairwise relatively prime. The solution x, $0 \le x \le M$, to $x = a_i \bmod m_i$ for $i = 1, 2, \ldots, r$ is given by

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M,$$

where $M_i = M/m_i$, and $y_i = M_i^{-1} \bmod m_i$.

Legendre and Jacobi Symbols:

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

The law of quadratic reciprocity (p, q primes)

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}$$

- $\left(\frac{q}{p}\right) = \left(\frac{q \bmod p}{p}\right)$
- $\left(\frac{q \cdot r}{p}\right) = \left(\frac{q}{p}\right) \cdot \left(\frac{r}{p}\right)$
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Computing square roots of a in $\mathbb{F}_p$: When $p = 3 \bmod 4$,

$$x = a^{(p+1)/4} \bmod p,$$

Ch 2:

For the curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (char K not 2 or 3), and $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, we have $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$. Also if $x_1 \neq x_2$ we set $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $\mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$. If $x_1 = x_2$ and $P_2 \neq -P_1$ we set $\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$, $\mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$. Now $P_1 + P_2 = P_3 = (x_3, y_3)$ is given by $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ and $y_3 = -(\lambda + a_1)x_3 - \mu - a_3$.

Ch 12:

Pohlig-Hellman: solving DLP $g^x = h$ in group of order N.

$S = \{\}$
forall primes p dividing N **do**
Compute largest $T = p^e$ dividing N
$g_1 = g^{N/T}$
$h_1 = h^{N/T}$
$z = \text{DLPOracle}(g_1, h_1, p^e)$
$S = S + \{(z, T)\}$
end
$x = CRT(S)$