

Math/Cmsc 456, Jeffrey Adams

Test II, May 8, 2009

SOLUTIONS

1. (a) Recall $L_3(xy) = L_3(x) + L_3(y)$. So $L_3(100) = L_3(2^2 5^2) = L_3(2) + L_3(2) + L_3(5) + L_3(5)$. This equals $72 + 72 + 87 + 87 = 66 \pmod{127}$.
(b) Note that $4 \times 17 = 68$, or $17 = 68 \times \frac{1}{4}$, which gives $L_3(17) = L_3(68) - L_3(4) = L_3(68) - L_3(2) - L_3(2) = 56 - 72 - 72 = 38 \pmod{127}$.

2. (a) By the formulas $m = \frac{3(3^2)+1}{2} = \frac{28}{2} = 14$. Note that $14 = -1 \pmod{15}$. Then $x_3 = 14^2 - 3 - 3 = -1 - 3 - 3 = -5 = 10 \pmod{15}$, and $y_3 = 14(3 - 10) - 1 = (-1)(-7) - 1 = 6 \pmod{15}$. So $Q = (10, 6)$.
(b) Adding $P + Q$ doesn't help, since $m = 5/7$ and 7 is invertible. Try $Q + Q$. Then $m = \frac{3(10^2)+1}{12}$. Since 12 is not invertible $\pmod{15}$ this gives a factorization. That is $GCD(15, 12) = 3$.
(c) The number of points N on the curve is divisible by the order of any point, so $68|N$. So $N = 68, 136, 204, \dots$. On the other hand by Hasse's theorem $|N - 128| < 2\sqrt{127} < 24$. So $N = 136$.

3. (a)

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \\ 1 & 4 & 16 & 64 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} -3 \\ 5 \\ 10 \\ 12 \end{pmatrix}$$

- (b) This is a Lagrange interpolation polynomial. Take $f_0(x) = (x - 1)(x - 2)(x - 3)$, so $f(1) = f(2) = f(3) = 0$, and this has degree 3. Then $x_0(4) = 6$, so divide by this to give

$$f(x) = \frac{1}{6}(x - 1)(x - 2)(x - 3).$$

Then $f(5) = 4$.

Note that

$$f(x) = -1 + \frac{11}{6}x - x^2 + \frac{1}{6}x^3$$

although this isn't necessary.

4. (a) If the password is y , compute $2^y \pmod{p}$ and compare it with the entry in the password file.
- (b) This is the discrete log problem. If Eve has the password file she knows $a = 2^x \pmod{p}$. To compute x means computing $L_2(a)$, which is hard.
- (c) Choose an elliptic curve E for a large prime p . Choose a point P on E . Both E and P can be made public. Then store xP in the password file. To check a password y , compute yP and see if it equals xP . This is secure based on the discrete log problem on E .
5. (a) If $a = p - 1$ then $\beta = \alpha^{p-a} = 1$, and this isn't secure. For example it is obvious what a is from α and β .
 Also note that $a = p - 1$ implies $a = 0 \pmod{p - 1}$ so that $s = k^{-1}m$. Then it is easy to recover k .
- (b) So that $k^{-1} \pmod{p - 1}$ is defined.
- (c) First write $m = sk + ar$. Then

$$\begin{aligned}
 \alpha^m &= \alpha^{sk+ar} \\
 &= \alpha^{sk} \alpha^{ar} \\
 &= (\alpha^k)^s (\alpha^a)^r = r^s \beta^r \pmod{p}
 \end{aligned}$$