Solutions to Assignment #5

5 a)+b) The slope of the tangent line to the curve is $\frac{3x^2}{2y}$ so is 2 at $(2,3)$ making the tangent line $y = 2x-1$. The third point on the line has x-coord satisfying

$(2x-1)^2 = x^3+1$ so $x(x-2)^2 = 0$ The third point is then $x=0$, $y=-1$ and when we reflect we get $(0,1)$

So $2(2,3) = (0,1)$. To compute $3(2,3)$, the slope between $(2,3)$ and $(0,1)$ is 1 and so the line between them is $y = x+1$. Solving for the third point we get

$(x+1)^2 = x^3+1$ so $x(x-2)(x+1) = 0$ and the third point on the line is $(-1,0)$. Since it is its own reflection we get that $(2,3)+(0,1)$ is $(-1,0)$ and that $2(-1,0) = 0$.

So $6(2,3) = 0$ but neither $2(2,3)$ nor $3(2,3) = 0$ so the order of $(2,3)$ is 6 which means that $n(2,3)$ are all distinct for $n=1,\dots 6$.

6. a) The slope of the tangent line is $\frac{3x^2}{2y}$ and so for $P=(10,9$ the slope is $50\cdot 3^{-1}$. Now the $\gcd(3,35)=1$ and $3^{-1}=12$. so the slope is $600 \equiv 5 \bmod 35$. The line is then $y = 5x+29$ or better $y=5x-6$. So we solve

$y^2 = (5x-6)^2 = x^3+26$ yielding $x^3-25x^2+10x-10 = 0$.

Two solutions of this are $x = 10$ and the third x, x_3 will satisfy $10 \cdot 10 \cdot (-x_3) = -10 \mod 35$ or $-10x_3 = 1 \mod 55$ But the gcd $(10, 35) = 5(!)$ and so we have found a factor of 35.

b) Repeating the above for $n = 35$, $y^2 = x^3 + 5x + 8$ and $P = (1, 28)$. The tgt. line has slope $\dfrac{3x^2+5}{2y}$ so at P is $\dfrac{8}{2 \cdot (-7)}$ but gcd $(7, 35) = 7$ and again we have found a factor.

9. As we noted in class, the Hasse Theorem gives us an upper bound on the number of points on an elliptic curve E over a field F. In fact,

$$|E(F)| \leq (q+1) + 2\sqrt{q} \quad \text{where } |F| = q.$$

So if in the Baby Step - Giant Step algorithm we let $N = [\sqrt{q+1+2\sqrt{q}}\,]$ and computed $g, g^2, g^3 \cdots g^N$ as well as $bg^{-N}, bg^{-2N}, \cdots bg^{-(N-1)N}$ then we may have computed too many elements of the elliptic curve then is necessary but we will definitely find a match by the argument in Chapter 7.

13. We prove this by induction w: If $w = 1$ and $b_1 = 0$ then $R_1 = S_1 = O$. If $b_1 = 1$ then $R_1 = S_1 + P = P$.

Now suppose that $R_w = xP$ whenever the binary length of x is $< k$.

Assume now that $x = b_1 b_2 \cdots b_{k-1} b_k$ and let

$x_0 = b_1 \cdots b_{k-1}$ so $2x_0 = b_1 b_2 \cdots b_{k-1} 0$ and by induction

$x_0 P = R_{w'}$ where the algorithm was applied to the sequence $b_1 \cdots b_{k-1}$. Then $2x_0 P = 2R_{w'} = S_k$ if $b_k = 0$. If $b_k = 1$ then we get $2x_0 P + P = 2R_{w'} + P = S_k$ which means $(2x_0 + 1)P = S_k$ and $2x_0 + 1 = x$.

b) Again we do this by induction, this time on a. If a is even then after the first step we are left with $a/2$, $\mathbf{O}$ and $2P$. By inductive assumption, the algorithm will produce $(a/2)2P = aP$.
If a is odd then after the first step, the algorithm ~~will~~ ~~produce~~ gives $a-1, P, P$ and the inductive assumption gives $(a-1)P + P = aP$.

16. a) The $\gcd(3, p-1)$ is either 1 or 3. If it is 3 then $3 | p-1$ so $p \equiv 1 \bmod 3$ but $p \equiv -1 \bmod 3$ meaning $\gcd(3, p-1) = 1$ i.e. 3 is invertible mod $p-1$ so there is some d s.t. $3d \equiv 1 \bmod p-1$.
b) If $a^3 \equiv b \bmod p$ then $a^{3d} \equiv b^d \bmod p$. But $3d \equiv 1 \bmod p-1$ so by Fermat, $a \equiv b^d \bmod p$. In the other direction, if $a \equiv b^d \bmod p$ then $a^3 \equiv b^{3d} \bmod p$ so $a^3 \equiv b \bmod p$ again by Fermat.
c) For $p \equiv -1 \bmod 3$, b) says that cube roots are unique. So for each value of $y^2 - 1$ there is only one x which will give this value. In F_p where $p \neq 2$, ~~every~~ $\frac{p+1}{2}$ ~~non-zero~~ elements have ~~two~~ square roots, - two for the non-zero elements and one for zero. This gives p points on the elliptic curve and adding the identity gives $p+1$.