

MATH 5405 - HW5

DUE WEDNESDAY APRIL 15

- 1) Factor 5251 using $p+1$ method. (The variant that uses gaussian integers.)
- 2) Show that if two numbers u and v satisfy $u^3 + v^3 = 1$ then the numbers

$$x = \frac{12}{u+v} \text{ and } y = 36 \frac{u-v}{u+v}$$

satisfy $y^2 = x^3 - 432$. Then use two obvious rational solutions of the equation $u^3 + v^3 = 1$ to find two not so obvious rational solutions of $y^2 = x^3 - 432$.

- 3) Let x_1, x_2 and x_3 be three zeros of the cubic polynomial $x^3 + bx + c$. Show that

$$-[(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2 = 4b^3 + 27c^2.$$

- 4) Let $P = (1, 3)$ be a point on the elliptic curve $y^2 = x^3 + 8$. Compute $2P$, $4P$ and $8P$.

- 5) Let $P = (1, 1)$ be a point on the degenerate cubic curve $y^2 = x^3$. Compute nP for $n = 1, 2, \dots, 5$. What do you think nP should be? If $nP = (x_n, y_n)$, what is x_n/y_n ?

- 6) Let $P = (2, 2)$ be a point on the degenerate cubic curve $y^2 = x^3 - x^2$. Compute $2P$ and $4P$.

- 7) Compute the order of the group $E(p)$ for $p = 17$ and $p = 19$, where E is the elliptic curve $y^2 = x^3 + 8$.

- 8) Compute the order of the point $P = (1, 3)$ on the curve $y^2 = x^3 + 8$ modulo 41.

- 9) Factor 7519 by doubling (as many times as necessary) the point $P = (2, 5)$ on the curve $y^2 = x^3 + 17$.

- 10) Factor 6077 using the point $P = (2, 5)$ on the curve $y^2 = x^3 + 17$. That is, compute $P_2 = 2P$, then $P_3 = 3P_2$ etc...