18.704 Fall 2004 Homework 9 Solutions

All references are to the textbook "Rational Points on Elliptic Curves" by Silverman and Tate, Springer Verlag, 1992. Problems marked **(*)** are more challenging exercises that are optional but not required.

1. A *Carmichael number* is an integer $n \geq 1$ such that $a^{n-1} \equiv 1 (\bmod n)$ holds for all a relatively prime to n. FYI: I believe the question of whether there exist infinitely many Carmichael numbers is an open problem.

(a) Suppose that $n = p_1 p_2 \dots p_r$ is a product of r *distinct* primes. Show that n is a Carmichael number if and only if $p_i - 1$ divides $n - 1$ for each i (hint: look up Fermat's Little Theorem and the Chinese Remainder Theorem if you don't know these.) Find a product of three distinct primes which is a Carmichael number (there exist several possibilities with all three primes less than 20.)

(b) Show that no product of two distinct primes is a Carmichael number.

Solution. (a). Suppose that $n = p_1 p_2 \dots p_r$, where the p_i are distinct primes, is a Carmichael number. For each i, the multiplicative group $\mathbb{F}_{p_i}^*$ of the finite field $\mathbb{F}_{p_i}$ is cyclic. This means for all a with $\gcd(a, p_i) = 1$, that $a^{p_i - 1} \equiv 1 (\bmod p_i)$ (Fermat's little theorem). Moreover, we can choose a *primitive root* g_i for each p_i; i.e. g_i is a number with $\gcd(g_i, p_i) = 1$ and such that $p_i - 1$ is the *minimal* nonzero integer m such that $a^m \equiv 1 (\bmod p_i)$ (i.e. g_i is a generator for the cyclic group $\mathbb{F}_{p_i}^*$.) Then by the Chinese Remainder Theorem, there is some integer g such that $g \equiv g_i (\bmod p_i)$ for all i. (In fancier language, the Chinese Remainder Theorem is just saying that the product group $\bigoplus_i \mathbb{Z}/p_i\mathbb{Z}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.) In particular, then, $\gcd(g, n) = 1$, and so $g^{n-1} \equiv 1 (\bmod n)$ by the definition of Carmichael number. Then for each i, $1 \equiv g^{n-1} \equiv g_i^{n-1} (\bmod p_i)$, and then $p_i - 1$ divides $n - 1$ by the definition of g_i.

Conversely, suppose that $p_i - 1 | n - 1$ for all i. Then if $\gcd(a, n) = 1$, in particular $\gcd(a, p_i) = 1$ for all i. So $a^{p_i - 1} \equiv 1 (\bmod p_i)$ by Fermat's little theorem, and then $a^{n-1} \equiv 1 (\bmod p_i)$ for each i. Finally, since the p_i are distinct primes this implies by the Chinese Remainder Theorem again that $a^{n-1} \equiv 1 (\bmod n)$.

To find a Carmichael number, one can just play around a bit. The smallest is $561 = (3)(11)(17)$.

(b). Suppose that $n = pq$ is a Carmichael number, where p and q are distinct primes. By part (a), this means that $p - 1$ and $q - 1$ both divide $pq - 1$. But we can write $pq-1 = pq-q+q-1 = q(p-1)+q-1$, and so $p-1$ divides $q-1$. A symmetric argument shows that $q-1$ divides $p-1$. But this can't happen unless $p-1 = q-1$, but then $p = q$ which is a contradiction.

Remark. As both Isabel Lugo and Jacob Fox pointed out, it is no longer an open problem whether there exist infinitely many Carmichael numbers. In fact there are a lot of them: for large n, there are at least $n^{2/7}$ Carmichael numbers less than or equal to n. For a summary of what is currently known about Carmichael numbers, see

http://mathworld.wolfram.com/CarmichaelNumber.html.

2. Do Exercise 5.5 (a) and (b).

Solution. (a) Let p be a prime; we are looking for integer solutions to $x^3+y^3 = p$. Factor $x^3+y^3 = (x+y)(x^2-xy+y^2)$.

For use in both this problem and problem 3 below, we prove a few facts about the factors appearing here. First of all, $x^2-xy+y^2 \geq 0$ for all $x, y \in \mathbb{Z}$. This is because $x^2-xy+y^2 \geq (x-y)^2$ if x and y have the same sign, and $x^2-xy+y^2 \geq (x+y)^2$ if x and y have different signs.

Next, we claim that for almost all $x, y \in \mathbb{Z}$ (with a few exceptions), $x+y < x^2-xy+y^2$. To prove this claim, first note that if x and y are both negative, we can just replace them by their opposites, so we might as well assume that at most one of x and y is negative, and by symmetry that one might as well be x. So we only have two cases:

Case 1: x, y both ≥ 0. If also $x > y$, then $x^2-xy+y^2 = x(x-y)+y^2 \geq x+y^2 \geq x+y$, with equality only if $(x,y) = (1,0)$ or $(2,1)$. If $y > x$, a symmetric argument gives $x^2-xy+y^2 \geq x+y$ with equality only if $(x,y) = (0,1)$ or $(1,2)$. If $x = y$, then $x^2 \geq 2x$ unless $(x,y) = (1,1)$, and equality occurs only if $(x,y) = (0,0)$ or $(2,2)$.

Case 2: $x < 0 \leq y$. In this case, $x^2-xy+y^2 = x^2+y(y-x) \geq x^2+y \geq x+y$. Note that equality never occurs here.

To summarize, we have shown the following:

Lemma 0.1 *Let $x, y \in \mathbb{Z}$. Then $x+y \leq x^2-xy+y^2$ unless $(x,y) = (1,1)$. Furthermore, equality occurs if and only if*

$$(x,y) \in \{(0,0),(0,1),(1,0),(2,1),(1,2),(2,2)\}.$$

Now back to Problem 2. Suppose that $(x+y)(x^2-xy+y^2) = p$ where p is prime. Then either $p = |x+y|$ and $|x^2-xy+y^2| = 1$ or $1 = |x+y|$ and $|x^2-xy+y^2| = p$. The first case is impossible by the Lemma unless $x = y = 1$ and $p = 2$. Note that if $p = 2$ then in fact $(1,1)$ is the only solution to $x^3+y^3 = 2$.

Assuming now that $p \neq 2$, we must have $|x+y| = 1$ and $|x^2-xy+y^2| = p$. Since we showed above that x^2-xy+y^2 is always nonnegative, $x+y = 1$ and $x^2-xy+y^2 = p$. Then substituting $y = 1-x$, we have $x^2-x(1-x)+(1-x)^2 = p$, and so $3x^2 - 3x + 1 = p$. In particular, setting $u = -x$, we see that $p = 3u^2 + 3u + 1$ has the required form. In this case $(-u, u+1)$ is a solution. Note that $3(-u-1)^2 + 3(-u-1) + 1 = 3u^2 + 3u + 1$, so we need not worry about negative u, as long as we also include the solution $(u+1, -u)$ for each positive u.

(b) The only positive u for which $3u^2 + 3u + 1$ is less than 300 are $u = 0, 1, 2, \ldots, 9$. The possible values for p we get in this range are 1,7,19,37,61,91,127,169,217, and 271. Only 7,19,37,61,127,271 are primes.

So for only 7 primes less than 300 does the equation have any solutions. These solutions are $(n, -n+1)$ and $(-n+1, n)$ for $n = 2, 3, 4, 5, 7, 10$, corresponding to the primes $7, 19, 37, 61, 127, 271$, and the additional solution $(1, 1)$ for the prime $p = 2$.

3. Do Exercise 5.4 from the text.

Solution. We are looking for solutions to the equation $x^3 + y^3 = m$, where we count (u, v) and (v, u) as distinct solutions if $u \neq v$. Let $d(m)$ be the number of distinct divisors of m.

Factor the equation to give $(x+y)(x^2 - xy + y^2) = m$. As we saw in Problem 2, $x^2 - xy + y^2$ is always nonnegative. So we must have a factorization $m = d_1 d_2$ with $d_1, d_2 \geq 0$ and $x + y = d_1$, $x^2 - xy + y^2 = d_2$. Moreover, by Lemma 0.1, $d_2 < d_1$ is possible only if $x = y = 1$, but then $m = 2$. We know that if $m = 2$ then $(1, 1)$ is the only solution, so there are certainly at most $d(2) = 2$ solutions.

So assume now that $m \geq 2$. Consider the exceptional points (x, y) in the list of Lemma 0.1 for which $x + y = x^2 - xy + y^2$. Given one of these points, we have $x + y \in \{0, 1, 3, 4\}$ and so $m \in \{0, 1, 9, 16\}$. $m = 0$ and $m = 1$ are not allowed by hypothesis. If $m = 9$, then we calculate by hand that $(1, 2)$ and $(2, 1)$ are the only solutions. If $m = 16$, we calculate that $(2, 2)$ is the only solution. So certainly there are at most $d(m)$ solutions for each of these m.

Finally, we consider $m \geq 2$, $m \neq 9, 16$. Then given any factorization $m = d_1 d_2$ with $x + y = d_1$, $x^2 - xy + y^2 = d_2$, it follows from Lemma 0.1 that in fact $d_1 < d_2$. There are at most $d(m)/2$ possible possible factorizations $m = d_1 d_2$ with $d_1 < d_2$. For each of them, substituting $y = d_1 - x$ into $x^2 - xy + y^2 = d_2$, we get a quadratic in x, which has at most 2 integer solutions for x, and then y is determined. So there at most 2 integer points corresponding to each of the $d(m)/2$ factorizations, and thus at most $d(m)$ possible integer points.