Math 105, Fall 2010, HW5

1. Find the order of $(0,3)$ in the elliptic curve group $E_{-1,2}(\mathbb{F}_7)$. What is the index of the subgroup generated by $(0,3)$ in the full elliptic curve group?

2. Show that if n is an odd number with exactly k distinct prime factors, then squaring is a $2^k : 1$ homomorphism on $(\mathbb{Z}/n\mathbb{Z})^*$.

3. Suppose n is an odd number and write $\varphi(n)$ as $2^u v$ where v is odd. We know from Euler's theorem that for any integer a coprime to n that $a^{2^u v} \equiv 1 \pmod{n}$. Let N denote the number of residues a $(\text{mod} n)$ where either

$$a^v \equiv 1 \pmod{n} \quad \text{or} \quad a^{2^i v} \equiv -1 \pmod{n}$$

for some $i < u$. Show that if n is divisible by at least 2 distinct primes, then $N < n/2$. (Hint: Pattern your proof on a similar result connected with strong pseudoprimes.)

4. Given n and $\varphi(n)$, describe a polynomial-time random algorithm to factor n. (Hint: Use the previous problem.)

5. In the RSA cryptosystem, there is a public modulus n which is the product of two primes p, q, which are not public. An encryption exponent E is a random number coprime to $\varphi(n)$, and it is public. A decryption exponent D is an integer with $DE \equiv 1 \pmod{\varphi(n)}$, and it is secret. It has the property that for every integer M, we have

$$M^{ED} \equiv M \pmod{n}.$$

Anyone who knows p, q can easily find D since it just involves finding the inverse of E modulo $(p-1)(q-1)$. Show conversely, if one has any integer D that satisfies the above displayed congruence for all M, then one can easily factor n. (Hint: Use an analog of the previous problem.)