Math 362 Assignment 4

Due: Wednesday, October 30

- Answer all questions. Each question is worth 5 marks. Full marks will be awarded only for answers that are both mathematically correct and coherently written.
- Please consider the markers and write neatly and legibly! I have instructed the markers to ignore work they cannot read. (And I won't read it, either.)

1. Your public key for the RSA encryption algorithm is $(1147, 463)$. Since you own the key, you know that $1147 = 31 \times 37$, hence you (should) know the secret decryption exponent j.

   (a) What is j?

   (b) SUMS (Students in Undergraduate Mathematics and Statistics Course Union) have organised a treasure hunt, in which they have hidden a new laptop computer in a house in a certain street in Greater Victoria. The first person to find the laptop can keep it. If they told you it was hidden in a house in 0904 0366 0406 1036 Avenue, where would you go to find it?

2. Given that 3 is a primitive root of 43, use Lemma 10.1 (and other arguments) to find

   (a) all integers $a \in \Phi(43)$ such that $\operatorname{ord}_{43} a = 6$,

   (b) all integers $a \in \Phi(43)$ such that $\operatorname{ord}_{43} a = 21$.

3. Let g be a primitive root of the odd prime p. Prove that

   (a) if $p \equiv 1 \pmod 4$, then $p - g$ is also a primitive root of p;

   (b) if $p \equiv 3 \pmod 4$, then $\operatorname{ord}_p(p - g) = \frac{p-1}{2}$.

4. How many primitive roots does 98 have? Find all of them. (That is, find one primitive root g, and then determine all exponents k such that the least residue of g^k is also a primitive root.)

5. Prove that if $n > 2$, then $\phi(n)$ is even. Proceed as follows.

   (a) Assume $n = 2^k$ for some $k \geq 2$ and prove that $\phi(n)$ is even.

   (b) Assume n is not a power of 2. Then n can be written as $n = p^k m$, where p is an odd prime, $k \geq 1$ and $(p, m) = 1$. Now show that $\phi(n)$ is even.

6. Show that if p is an odd prime, then g is a primitive root of p if and only if exactly one of g and $g + p$ is a primitive root of $2p$. Proceed as follows.

   (a) Show that $\phi(2p) = \phi(p)$.

(b) Show that if g is a primitive root of p, then g is a primitive root of $2p$ if and only if g is odd, while $g+p$ is a primitive root of $2p$ if and only if g is even. (The Binomial Theorem might be useful.)

7. Solve the quadratic congruence $5x^2 + 6x + 1 \equiv 0 \pmod{23}$. Show your work. No marks for trying all least residues of 23!