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?

   Answer

   (a) $j = 7$

   (b) Parker Avenue.

2. Given that 3 is a primitive root of 43, find

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

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

   Answer

   (a) Since 43 is prime, $\phi(43) = 42$. Since 3 is a primitive root of 43, $\operatorname{ord}_{43} 3 = 42$. Consider 3^7. Since 3 is a primitive root, none of 3^7, $(3^7)^2$, $(3^7)^3$ is congruent to 1 (mod 43), while $(3^7)^6 \equiv 3^{42} \equiv 1 \pmod{43}$. Therefore, $\operatorname{ord}_{43} 3^7 = 6$. By Lemma 10.1, $(3^7)^k$, where $1 \le k \le 6$, has order 6 if and only if $(k, 6) = 1$, that is, if and only if $k = 1$ or $k = 5$.

   Therefore, all integers $a \in \Phi(43)$ such that $\operatorname{ord}_{43} a = 6$ consist of the least residues, modulo 43, of 3^7 and 3^{35}.

(b) Consider 3^2. Then none of $(3^2)^1$, $(3^2)^3$, $(3^2)^6$, $(3^2)^7$, $(3^2)^{14}$ is congruent to $1 \pmod{43}$, while $(3^2)^{21} \equiv 3^{42} \equiv 1 \pmod{43}$. Therefore, $\mathrm{ord}_{43} 3^2 = 21$. By Lemma 10.1, $(3^2)^k$, where $1 \le k \le 21$, has order 21 if and only if $(k, 21) = 1$, that is, if and only if $k \in \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

Therefore, all integers $a \in \Phi(43)$ such that $\mathrm{ord}_{43} a = 21$ consist of the least residues, modulo 43, of 3^{2k}, where $k \in \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

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 $\mathrm{ord}_p(p - g) = \frac{p-1}{2}$.

Answer

(a) Say $p = 4k+1$ for some integer $k \ge 1$. Since p is prime, $\phi(p) = 4k$, hence $\mathrm{ord}_p g = 4k$ because g is a primitive root. Since $g \in \Phi(p)$, we have that $(p - g, p) = 1$, hence $p - g \in \Phi(p)$. Let $t = \mathrm{ord}_p(p - g)$. We have to show that $t = 4k$.

By Fermat's theorem, $(p-g)^{4k} \equiv 1 \pmod p$. By Theorem 10.1 applied to $p - g$, $t | 4k$.

Suppose first that t is odd. Then $(t, 4) = 1$, hence $t | k$. Now

$$(p - g)^{2t} \equiv (-g)^{2t} \equiv (-1)^{2t} g^{2t} \equiv g^{2t} \pmod p.$$

However, by definition of t,

$$(p - g)^{2t} \equiv ((p - g)^t)^2 \equiv 1 \pmod p.$$

Therefore we have that

$$g^{2t} \equiv 1 \pmod p.$$

By Theorem 10.1 applied to g, $4k | 2t$, that is, $2k | t$, which is impossible since $t | k$.

Now suppose that t is even. Then

$$1 \equiv (p - g)^t \equiv (-g)^t \equiv g^t \pmod p.$$

Again by Theorem 10.1, $4k | t$. Since $t \le 4k = \phi(p)$, it follows that $t = 4k$. This shows that $p - g$ is also a primitive root of p.

(b) Say $p = 4k + 3$ for some integer $k \ge 1$ and let $t = \mathrm{ord}_p(p - g)$. Note that $\phi(p) = 4k + 2$. By Fermat's Theorem, $g^{4k+2} \equiv 1 \pmod p$. The quadratic congruence

$$g^{4k+2} \equiv (g^{2k+1})^2 \equiv 1 \pmod p$$

and the fact that $\mathrm{ord}_p g = 4k + 2$ imply that $g^{2k+1} \equiv -1 \pmod p$, therefore

$$(-g)^{2k+1} \equiv -g^{2k+1} \equiv 1 \pmod p.$$

By Theorem 10.1 applied to $-g$, $t|(2k+1)$ and so $2t|(4k+2)$. Now

$$g^{2t} \equiv (-g)^{2t} \equiv ((-g)^t)^2 \equiv 1 \pmod{p},$$

so by Theorem 10.1 applied to g, $(4k+2)|2t$. Therefore $4k+2 = 2t$, that is, $t = 2k+1$ as required.

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.)

Answer

Since $98 = 2 \times 7^2$, Theorem 10.7 implies that 98 has primitive roots, hence it has $\phi(\phi(98)) = \phi(42) = 12$ primitive roots. Finding the smallest primitive root of 98 is done by trial and error. Let us try $3 \in \Phi(98)$ first. We only need to check powers r of 3 that are divisors of 42, that is, $r \in \{1, 2, 3, 6, 7, 14, 21, 42\}$. Of these numbers, 6 is the smallest exponent r such $3^r > 98$, we only need to check powers $r \in \{6, 7, 14, 21\}$. Since

$$\begin{aligned}
3^6 &\equiv 43 \pmod{98}, \\
3^7 &\equiv 31 \pmod{98}, \\
3^{14} &\equiv 79 \pmod{98}, \\
3^{21} &\equiv 97 \equiv -1 \pmod{98},
\end{aligned}$$

we deduce that 3 is a primitive root of 98 (5 is another small primitive root.)

By Lemma 10.1, 3^k has order 42 if and only if $k \in \Phi(42)$, that is, if and only if $k \in S = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}$. The primitive roots of 98 are the least residues of the numbers $3^k \pmod{98}$, where $k \in S$.

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.

Answer

(a) Since $n = 2^k$, $\phi(n) = 2^k \cdot \frac{1}{2} = 2^{k-1}$. But $k \geq 2$ because $n > 2$, therefore 2^{k-1} is even.

(b) Since $n = p^k m$ where $(p,m) = 1$, we also have that $(p^k, m) = 1$. Since ϕ is multiplicative,

$$\phi(n) = \phi(p^k m) = \phi(p^k)\phi(m) = p^{k-1}(p-1)\phi(m).$$

Since p is odd, $p-1$ is even and so $\phi(n)$ 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.)

Answer

(a) Since ϕ is multiplicative and $(2,p) = 1$, $\phi(2p) = \phi(2)\phi(p) = \phi(p) = p-1$.

(b) Suppose g is a primitive root of p. Assume first that g is odd. Then $(g, 2p) = 1$ since $(g,p) = 1$ and $(g,2) = 1$. Hence $\operatorname{ord}_{2p} g$ is defined.

Suppose $\operatorname{ord}_{2p} g = t$. Then $g^t \equiv 1 \pmod{2p}$, that is, $g^t = (2p)k + 1$ for some integer k, so $g^t \equiv 1 \pmod{p}$.

By Theorem 10.1, $\operatorname{ord}_p g | t$. Since g is a primitive root of p, $\operatorname{ord}_p g = \phi(p)$. Therefore, $\phi(p)|t$. But by (a), $\phi(p) = \phi(2p)$, hence $\phi(2p)|t$. By Theorem 10.2 we also have that $t|\phi(2p)$. Hence $t = \phi(2p)$ from which it follows (by definition of $\operatorname{ord}_{2p} g$ and primitive roots) that g is a primitive root of $2p$.

Assume next that g is even. Then $(g, 2p) \geq 2$, hence $\operatorname{ord}_{2p} g$ is not defined and g is not a primitive root of $2p$.

On the other hand, since $(g,p) = 1$ and $g+p$ is odd, $(p+g, 2p) = 1$. Hence $\operatorname{ord}_{2p}(p+g)$ is defined. Moreover, $p+g$ is a least residue of $2p$. Suppose $\operatorname{ord}_{2p}(g+p) = t$. Then

$$(g+p)^t \equiv 1 \pmod{2p}.$$

By the Binomial Theorem,

$$(g+p)^t = \sum_{i=0}^{t} \binom{t}{i} g^i p^{t-i} = p^t + \binom{t}{1} g p^{t-1} + \cdots + \binom{t}{t-1} g^{t-1} p + g^t.$$

Since g is even, $2p | g^i p^{t-i}$ for each $i = 1, ..., t-1$, from which we get that

$$1 \equiv (g+p)^t \equiv p^t + g^t \pmod{2p}.$$

Therefore

$$p^t + g^t = (2p)k + 1 = (2k)p + 1$$

for some integer k. Hence

$$p^t + g^t \equiv g^t \equiv 1 \pmod{p}.$$

Again it follows that $t = \phi(p) = \phi(2p)$. By the definitions of $\mathrm{ord}_{2p}(g+p)$ and primitive roots, $g + p$ is a primitive root of $2p$.

Since $\phi(2p) = \phi(p)$, we also have that $\phi(\phi(p)) = \phi(\phi(2p))$. Hence we have shown that there is a one-to-one correspondence between the primitive roots of p and $2p$, from which the result follows.

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!

Answer

Since $14 \cdot 5 \equiv 1 \pmod{23}$, we begin by multiplying the congruence with 14 to obtain

$$x^2 + 15x + 14 \equiv 0 \pmod{23}.$$

that is,

$$x^2 - 8x + 14 \equiv 0 \pmod{23}.$$

Completing the square, we get

$$x^2 - 8x + 16 \equiv 2 \pmod{23},$$

or

$$(x-4)^2 \equiv 2 \equiv 25 \equiv 5^2 \pmod{23}.$$

Therefore, $x - 4 \equiv 5$ or $18 \pmod{23}$, from which it follows that $x = 9$ or $x = 22$.