Math 223, Spring 2009
Final Review Solutions

(1) Determine whether the following congruences have a solution.
   (a) $x^2 + 1 \equiv 0 \pmod{6911}$
   (b) $x^2 + 6x + 10 \equiv 0 \pmod{19}$

Solution:
   (a) Since $6911 \equiv 3 \pmod 4$, this equation has no solutions by Quadratic Reciprocity Part 1.
   (b) Completing the square gives $(x+3)^2+1 \equiv 0 \pmod{19}$ or $(x+3)^2 \equiv -1 \pmod{19}$. Since $19 \equiv 3 \pmod 4$, this equation has no solution, again by Quadratic Reciprocity Part 1.

(2) Compute $\left(\frac{84}{103}\right)$ and $\left(\frac{24}{31}\right)$.

Solution: For the first Legendre symbol, we have

$$\left(\frac{84}{103}\right) = \left(\frac{2^2 \cdot 3 \cdot 7}{103}\right) = \left(\frac{3 \cdot 7}{103}\right) = \left(\frac{3}{103}\right)\left(\frac{7}{103}\right).$$

Since 103, 3, and 7 are all congruent to 3 mod 4, we get

$$\left(\frac{3}{103}\right)\left(\frac{7}{103}\right) = -\left(\frac{103}{3}\right) \cdot -\left(\frac{103}{7}\right) = \left(\frac{1}{3}\right)\left(\frac{5}{7}\right).$$

Now since 1 is always a quadratic residue mod p and since $5 \equiv 1 \pmod 4$, the last product of Legendre symbols can be rewritten as

$$\left(\frac{1}{3}\right)\left(\frac{5}{7}\right) = \left(\frac{5}{7}\right)\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right).$$

Finally, by Quadratic Reciprocity Part 2, we have $\left(\frac{2}{5}\right) = -1$ as $5 \equiv 5 \pmod 8$.

For the second Legendre symbol, after factoring and observing that $31 \equiv 7 \pmod 8$ so we can use Quadratic Reciprocity Part 2, we have

$$\left(\frac{24}{31}\right) = \left(\frac{2^3 \cdot 3}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{3}{31}\right) = 1 \cdot \left(\frac{3}{31}\right) = \left(\frac{3}{31}\right).$$

Now since $31 \equiv 3 \pmod 4$ and $3 \equiv 3 \pmod 4$,

$$\left(\frac{3}{31}\right) = \left(\frac{31}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

(3) Let p be an odd prime and let a be a quadratic residue mod p. Prove that, if $p \equiv 1 \pmod 4$, then $p - a$ is also a quadratic residue mod p, but that, if $p \equiv 3 \pmod 4$, then $p - a$ is a nonresidue mod p.

Solution: Since $p - a \equiv -a \pmod p$, we have

$$\left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right).$$

By Quadratic Reciprocity Part 1, $\left(\frac{-1}{p}\right)$ depends on whether p is congruent to 1 or 3 modulo 4 exactly in the desired way.

(4) Show that another way to state the last part of Quadratic Reciprocity is the following: If p and q are distinct odd primes, then

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$$

Solution: If either p or q is congruent to 1 mod 4, say p is, then $p = 4k+1$ for some $k \in \mathbb{N}$ and thus

$$(-1)^{(p-1)(q-1)/4} = (-1)^{(4k+1-1)(q-1)/4} = (-1)^{k(q-1)} = 1$$

since q is odd and $q-1$ is even. It follows that $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ must have the same sign.

If both p and q are congruent to 3 mod 4, then $p = 4k+3$ and $q = 4l+3$ for some $k, l \in \mathbb{N}$, and so

$$(-1)^{(p-1)(q-1)/4} = (-1)^{(4k+2)(4l+2)/4} = (-1)^{4k^2+2k+2l+1} = -1$$

since the exponent is always odd. Thus $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ must have opposite signs.

(5) Let p be an odd prime. Prove that there are $\frac{p-1}{2} - \phi(p-1)$ quadratic nonresidues of p that are not primitive roots of p.

Solution: For p an odd prime, there exists a primitive root g and the $\frac{p-1}{2}$ nonresidues are given by $g, g^3, g^5, ..., g^{p-2}$. Also recall that, if g^k is a primitive root, then $gcd(k, p-1) = 1$, so in particular, all the primitive roots are in the above list. Since there are $\phi(p-1)$ primitive roots, the result follows.

(6) Prove that, if p is a Fermat prime, then every quadratic nonresidue of p is also a primitive root of p. (Recall that a Fermat prime has the form $2^{2^n}+1$ for some $n \in \mathbb{N}$.)

Solution: Let $p = 2^{2^n}+1$ be a Fermat prime for some $n \in \mathbb{N}$. Suppose $\left(\frac{a}{p}\right) = -1$, so that $a^{(p-1)/2} \equiv -1 \pmod{p}$. Note that the only prime that divides $p-1$ is 2. Since $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, we conclude that a is a primitive root mod p.

(7) Use Euclidean algorithm to find the inverse of 23 mod 26 and the inverse of 8 mod 13.

Solution: Since $gcd(23, 26) = 1$, inverse exists. To find it, we solve $23u + 26v = 1$. Euclidean algorithm gives a solution $(u, v) = (-9, 8)$. Thus $u = -9$ is a desired inverse, or, if we take the least positive residue mod 26, the answer is 17.

For the second part, we similarly get that the inverse of 8 modulo 13 is 5.

(8) Affine transformation cipher $C \equiv 7P+10 \pmod{26}$ was used to encode a message. The encrypted message is $LJMKGMGMFXQEXMV$. Find the plaintext message. (Use $A = 0$, $B = 1$, ..., $Z = 25$.)

Solution: To decrypt, we solve for P to get

$$P \equiv \overline{a}(C-b) \pmod{26}.$$

Here $\overline{a}$ is the inverse of a modulo 26.

For $a = 7$, it is not hard to see by inspection that $\overline{a} = 15$, so the decryption formula is

$$P \equiv 15(C-10) \pmod{26}.$$

The plaintext then comes out to be

$$PLEASESENDMONEY$$

(9) Decode the following using the Vigenère cipher and codeword $BETTERGRADE$:

$$JEVVIGZSRLFFWNGHVXKHHFSMWZIRZDIGRJKAM$$

Solution: Plaintext is

$$IACCEPTBRIBESUNDERTHEBRIDGEATMIDNIGHT$$

(10) RSA encryption with public key $(e, n) = (13, 2537)$ was used to encrypt a message. Ciphertext is 009516481410. If you know that the blocklength that was used is 4, find plaintext. (Use the $A = 00$, $B = 01$, ..., $Z = 25$.)

Solution: Since 2537 is easily factored as $43 \cdot 59$, it is not hard to decipher the message. The inverse of 13 mod $\phi(2537) = 42 \cdot 58$ is easily found to be 937. Then each block of the plaintext is recovered by $P \equiv C^{937} \pmod{2537}$. Using successive squaring, the plaintext blocks are found to be $1520 \equiv 95^{937} \pmod{2537}$, $0111 \equiv 1648^{937} \pmod{2537}$, and $0802 \equiv 1410^{937} \pmod{2537}$. The plaintext is thus 152001110802 and the corresponding plaintext is $PUBLIC$.

(11) Suppose Alice and Bob want to choose a key using use Diffie-Hellman key exchange. They publicly agree on the prime $p = 7$ and a primitive root $b = 3$. If Alice privately chooses $r = 12$ and Bob privately chooses $q = 9$, what is the key they would agree on?

Solution: The key is $1 \equiv (3^{12})^9 \equiv (3^9)^{12} \pmod{7}$ (not hard to compute using Fermat's Little Theorem).