Exam 2, Math 407 — Solutions

Problem 1. a) Define the Legendre symbol and the Jacobi symbol. State the quadratic reciprocity law.
b) Is the congruence $x^2 - 14x + 30 \equiv 0 \pmod{91}$ solvable?
c) Find all solutions to $7x^2 - 2x - 7 \equiv 0 \pmod{41}$.

Solution.

(a) Let p be an odd prime and . an integer. The *Legendre symbol* is

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \text{ is divisible by p,} \\ 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

Equivalently, $\left(\frac{a}{p}\right)$ is the unique element from $\{-1, 0, 1\}$ such that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Let n be a positive odd integer with prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$, and let a be any integer. The *Jacobi symbol* is

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Note: $\left(\frac{a}{n}\right) = 1$ does *not* guarantee that a is a QR mod n.

Quadratic Reciprocity. Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Equivalently, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless both $p \equiv q \equiv 3 \pmod{4}$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.
There are also the supplementary laws: $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ and $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

For computations of Legendre symbol the following extension, called Jacobi's Quadratic reciprocity, is very useful.

Jacobi's Quadratic Reciprocity. Let $m > 1$, $n > 1$ be odd integers. Then

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right).$$

Equivalently, $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ unless both $m \equiv n \equiv 3 \pmod{4}$, in which case $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$. There are also the supplementary laws: $\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}$ and $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$.

(b) We check solvability of $x^2 - 14x + 30 \equiv 0 \pmod{97}$. Complete the square:

$$(x-7)^2 \equiv 49 - 30 = 19 \pmod{97}.$$

We compute the Legendre symbol $\left(\frac{19}{97}\right)$. By the properties of Legendre symbol,

$$\left(\frac{19}{97}\right) = \left(\frac{97}{19}\right) = \left(\frac{5 \cdot 19 + 2}{19}\right) = \left(\frac{2}{19}\right) = -1.$$

Thus 19 is a quadratic non-residue mod 97, and the congruence has **no solutions**.

Alternatively, we compute the discriminant $\Delta = 14^2 - 4 \cdot 30 = 76 = 4 \cdot 19$ and use the fact that the congruence is solvable if and only Δ is a square modulo 97. As in the first solution,

$$\left(\frac{4 \cdot 19}{97}\right) = \left(\frac{2}{97}\right)^2 \left(\frac{19}{97}\right) = -1$$

so Δ is a quadratic non-residue mod 97, and the congruence has **no solutions**.

(c) We solve $7x^2 - 2x - 7 \equiv 0 \pmod{41}$. Multiply both sides by 7:

$$49x^2 - 14x - 49 = (7x - 1)^2 - 50 \equiv 0 \pmod{41}.$$

Since $50 \equiv 9 \pmod{41}$, this gives $(7x - 1)^2 \equiv 9 = 3^2 \pmod{41}$. Hence $7x - 1 \equiv \pm 3 \pmod{41}$, giving $7x \equiv 4$ or $7x \equiv -2 \pmod{41}$.

Since $7 \cdot 6 = 42 \equiv 1 \pmod{41}$), we recover $x \equiv 6 \cdot (7x)$:

- $7x \equiv 4$: $x \equiv 6 \cdot 4 = 24 \pmod{41}$.
- $7x \equiv -2$: $x \equiv 6 \cdot (-2) = -12 \equiv 29 \pmod{41}$.

Verification. For $x = 24$: $7(576) - 2(24) - 7 = 4032 - 48 - 7 = 3977 = 97 \cdot 41$.✓
For $x = 29$: $7(841) - 2(29) - 7 = 5887 - 58 - 7 = 5822 = 142 \cdot 41$.✓

The solutions are $\boxed{x \equiv 24 \pmod{41}}$ and $\boxed{x \equiv 29 \pmod{41}}$.

Problem 2. a) What does it mean that (a, b, c) is a primitive Pythagorean triple? Describe all such triples.
b) Find a primitive Pythagorean triple of the form $(a, b, 33)$, or prove none exists.
c) Find a primitive Pythagorean triple of the form $(a, b, 37)$, or prove none exists.

Solution.

(a) A *Pythagorean triple* (a, b, c) of positive integers satisfies $a^2 + b^2 = c^2$. It is *primitive* if $\gcd(a, b) = \gcd(a, b) = \gcd(a, b) = 1$.

Classification. In every primitive Pythagorean triple c is odd and one of a, b is even. Every primitive Pythagorean triple with b even has the form

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

where $m > n > 0$, $\gcd(m, n) = 1$, and $m \not\equiv n \pmod{2}$ (i.e. m and n have opposite parity). Every such choice produces a distinct primitive triple. Note that in any primitive triple the hypotenuse c is odd and its prime factors are all congruent to $1 \pmod{4}$.

(b) We show no primitive Pythagorean triple with hypotenuse 33 exists.

In a primitive triple the hypotenuse has the form $c = m^2 + n^2$. A positive integer is a sum of two squares if and only if every prime $p \equiv 3 \pmod{4}$ appears to an even power in its factorisation. Now $33 = 3 \cdot 11$; both $3 \equiv 3 \pmod{4}$ and $11 \equiv 3 \pmod{4}$ appear to the first (odd) power. Therefore 33 is *not* a sum of two squares, and no primitive Pythagorean triple with hypotenuse 33 exists.

(c) Since $37 \equiv 1 \pmod 4$, the prime 37 is a sum of two squares. Indeed $37 = 36 + 1 = 6^2 + 1^2$. Taking $m = 6$, $n = 1$ (note $\gcd(6, 1) = 1$ and they have opposite parity), the classification gives the primitive triple

$$a = m^2 - n^2 = 35, \quad b = 2mn = 12, \quad c = m^2 + n^2 = 37.$$

Verification: $35^2 + 12^2 = 1225 + 144 = 1369 = 37^2$.✓

The primitive Pythagorean triple is $\boxed{(35,\ 12,\ 37)}$.

Problem 3. Find positive integers a, b such that $61 \cdot 89 = a^2 + b^2$.

Solution. We use the identity: $(x^2 + y^2)(u^2 + v^2) = (xu - yv)^2 + (xv + yu)^2 = (xu + yv)^2 + (xv - yu)^2$.

Since $61 \equiv 1 \pmod 4$ and $89 \equiv 1 \pmod 4$, both primes are sums of two squares:

$$61 = 5^2 + 6^2, \qquad 89 = 5^2 + 8^2.$$

Applying the identity with $(x, y) = (5, 6)$ and $(u, v) = (5, 8)$:

$$\begin{aligned} 61 \cdot 89 &= (5^2 + 6^2)(5^2 + 8^2) \\ &= (5 \cdot 5 - 6 \cdot 8)^2 + (5 \cdot 8 + 6 \cdot 5)^2 = (-23)^2 + 70^2 = 529 + 4900, \\ &= (5 \cdot 5 + 6 \cdot 8)^2 + (5 \cdot 8 - 6 \cdot 5)^2 = 73^2 + 10^2 = 5329 + 100. \end{aligned}$$

Both give $5429 = 61 \cdot 89$ (check: $61 \cdot 89 = 61 \cdot 90 - 61 = 5490 - 61 = 5429$).

Two solutions are $\boxed{(a, b) = (23, 70)}$ and $\boxed{(a, b) = (10, 73)}$.

Problem 4. John spent \$510 on two kinds of posters: for \$15 and for \$31 each. What is the smallest number of posters he could get?

Solution. Let x be the number of \$15 posters and y the number of \$31 posters, with $x, y \geq 0$ integers. We need

$$15x + 31y = 510.$$

We minimise $x + y$. Since $15x = 510 - 31y$, we need $510 - 31y \geq 0$, i.e. $y \leq 510/31 \approx 16.45$, so $y \leq 16$. Also $15 \mid (510 - 31y)$. Since $510 = 34 \cdot 15$ we have $510 \equiv 0 \pmod{15}$, and $31 \equiv 1 \pmod{15}$, so the condition becomes $y \equiv 0 \pmod{15}$.

The non-negative values of y satisfying this are $y = 0$ and $y = 15$ (since $y = 30$ exceeds 16).

- $y = 0$: $x = 34$, total $= 34$ posters.
- $y = 15$: $31 \cdot 15 = 465$, $x = (510 - 465)/15 = 3$, total $= 3 + 15 = 18$ posters.

The minimum is $\boxed{18}$ posters (3 at \$15 and 15 at \$31).
Check: $3 \cdot 15 + 15 \cdot 31 = 45 + 465 = 510$.✓

Alternatively, one can follow the strategy from the solution to problem 4 from homework 9.

Problem 5. a) Prove that for any integer a we have $a^5 \equiv -1, 0, 1 \pmod{11}$.
b) Prove that $x^5 - 3y^5 = 5$ has no integer solutions.

Solution.

(a) If $11 \mid a$ then $a^5 \equiv 0 \pmod{11}$. If $11 \nmid a$, then by Fermat's Little Theorem $a^{10} \equiv 1 \pmod{11}$, so $(a^5)^2 \equiv 1 \pmod{11}$, meaning $a^5 \equiv \pm 1 \pmod{11}$. Hence for every integer a, $a^5 \equiv -1, 0, \text{or } 1 \pmod{11}$.

(b) Suppose x, y are integers with $x^5 - 3y^5 = 5$. We work modulo 11. By part (a), $x^5 \equiv \varepsilon_1$ and $y^5 \equiv \varepsilon_2$ where $\varepsilon_1, \varepsilon_2 \in \{-1, 0, 1\}$. The possible values of $x^5 - 3y^5 \pmod{11}$ are:

$$\varepsilon_1 - 3\varepsilon_2 \in \{1-3(1),\ 1-0,\ 1-3(-1),\ 0-3(1),\ 0,\ 0-3(-1),\ -1-3(1),\ -1-0,\ -1-3(-1)\},$$

which simplifies to $\{-2, -1, 0, 1, 2, 3, -4\} = \{7, 8, 9, 10, 0, 1, 2, 3, 4\} \pmod{11}$.

The value 5 (mod 11) is *not* in this set (the set contains $\{0, 1, 2, 3, 4, 7, 8, 9, 10\}$ but not 5 or 6). Therefore $x^5 - 3y^5 \equiv 5 \pmod{11}$ is impossible, and the equation has no integer solutions.

Problem 6. a) Define perfect numbers. What can you say about even perfect numbers?
b) Prove that if $k > 1$ and $m > 1$ are integers then $\sigma(km) > k\sigma(m)$.
c) Use (b) to show that if m, n are perfect numbers and $m \mid n$ then $m = n$.

Solution.

(a) A positive integer n is *perfect* if $\sigma(n) = 2n$, i.e. the sum of all its positive divisors equals twice itself (or equivalently, the sum of its proper divisors equals n).

Even perfect numbers (Euler–Euclid theorem). An even number n is perfect if and only if

$$n = 2^{p-1}(2^p - 1),$$

where p is a prime such that $2^p - 1$ is also prime (a *Mersenne prime*). Examples: $p = 2$ gives $n = 6$; $p = 3$ gives $n = 28$; $p = 5$ gives $n = 496$.

(b) Let $k > 1$ and $m > 1$. For each divisor $d \mid m$ we have $kd \mid km$, so the map $d \mapsto kd$ injects the divisors of m into the divisors of km. Therefore

$$\sigma(km) \ \geq \ \sum_{d \mid m} kd \ = \ k\sigma(m).$$

It remains to show strict inequality. Since km is a positive integer, $1 \mid km$, so 1 is a divisor of km. However, for any $d \mid m$ we have $kd \geq k \cdot 1 = k > 1$ (since $k > 1$), so $1 \notin \{kd : d \mid m\}$. Hence 1 contributes an additional positive term to $\sigma(km)$ beyond $k\sigma(m)$, giving

$$\sigma(km) > k\sigma(m).$$

(c) Let m and n be perfect numbers with $m \mid n$. Write $n = km$ for some positive integer k. We want to show $k = 1$, i.e. $m = n$.

Suppose for contradiction that $k > 1$ (and note $m > 1$ since m is perfect, so $m \geq 6$). By part (b),

$$\sigma(n) = \sigma(km) > k\sigma(m) = k \cdot 2m = 2km = 2n,$$

so $\sigma(n) > 2n$. But n is perfect, so $\sigma(n) = 2n$, a contradiction. Therefore $k = 1$ and $m = n$.

Problem 7. a) Define the Möbius function. State the Möbius inversion formula.
b) We know that $n^2 = \sum_{d \mid n} f(d)$ for all n. What is $f(9)$?
c) What is $\sigma * \phi(15)$?

Solution.

(a) The *Möbius function* $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ is a product of } k \text{ distinct primes}, \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p. \end{cases}$$

Möbius Inversion Formula. If F and f are arithmetic functions related by $F(n) = \sum_{d|n} f(d)$, then

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, F(d) = \sum_{d|n} \mu(d)\, F\Big(\frac{n}{d}\Big).$$

(b) We are given $n^2 = \sum_{d|n} f(d)$, so by Möbius inversion with $F(n) = n^2$:

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, d^2.$$

For $n = 9$ the divisors are $1, 3, 9$:

$$\begin{aligned} f(9) &= \mu(9) \cdot 1^2 + \mu(3) \cdot 3^2 + \mu(1) \cdot 9^2 \\ &= 0 \cdot 1 + (-1) \cdot 9 + 1 \cdot 81 \\ &= \boxed{72}. \end{aligned}$$

(We used $\mu(9) = \mu(3^2) = 0$, $\mu(3) = -1$, $\mu(1) = 1$.)

(c) We compute the convolution $(\sigma * \phi)(15) = \sum_{d|15} \sigma(d)\, \phi(15/d)$.

The divisors of 15 are $1, 3, 5, 15$. Relevant values:

d	1	3	5	15
$\sigma(d)$	1	4	6	24
$\phi(15/d)$	$\phi(15) = 8$	$\phi(5) = 4$	$\phi(3) = 2$	$\phi(1) = 1$
$\sigma(d)\phi(15/d)$	8	16	12	24

(We have $\sigma(15) = (1+3)(1+5) = 24$ and $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$.)

Therefore

$$(\sigma * \phi)(15) = 8 + 16 + 12 + 24 = \boxed{60}.$$

Remark. One can show in general that $\sigma * \phi = n \cdot \tau$ (i.e. $(\sigma * \phi)(n) = n\,\tau(n)$ where τ counts divisors), which gives $(\sigma * \phi)(15) = 15 \cdot 4 = 60$ as a quick check.✓

Optional Problems

Problem 8. Prove that the only solution to $x^5 - 3y^5 = 5z^5$ in integers is $x = y = z = 0$.

Solution. We use the same mod-11 analysis as in Problem 5, combined with infinite descent.

Step 1: We show that $11 \mid x$, $11 \mid y$, $11 \mid z$. If $11 \nmid z$, then z has an inverse u modulo 11 and multiplying the congruence $x^5 - 3y^5 \equiv 5z^5 \pmod{11}$ by u^5 we get

$$(ux)^5 - 3(uy)^5 \equiv 5(uz)^5 \equiv 5 \pmod{11}.$$

In our solution to Problem 5(b) we proved that the last congruence is not possible. Thus we must have $11 \mid z$. It follows that $x^5 \equiv 3y^5 \pmod{11}$.

If $11 \nmid y$, then y has an inverse w modulo 11 and multiplying the congruence $x^5 \equiv 3y^5 \pmod{11}$ by w^5 we get

$$(wx)^5 \equiv 3(wy)^5 \equiv 3 \pmod{11}.$$

By Problem 5(a), the last congruence is not possible. Hence $11 \mid y$.

We showed that $11 \mid z$ and $11 \mid y$. The equality $x^5 - 3y^5 = 5z^5$ implies now that $11 \mid x$.

Step 2: Infinite descent. Write $x = 11x'$, $y = 11y'$, $z = 11z'$. From $x^5 - 3y^5 = 5z^5$ we get

$$11^5(x')^5 - 3 \cdot 11^5(y')^5 = 5 \cdot 11^5(z')^5.$$

Dividing by 11^5 gives $(x')^5 - 3(y')^5 = 5(z')^5$. The same argument applies to (x', y', z'), showing $11 \mid x'$, $11 \mid y'$, $11 \mid z'$. By infinite descent, the only integer solution is $x = y = z = 0$. (A different way to phrase the solution is to assume the equation has non-zero solutions and choose one x, y, z with smallest possible $|x| + |y| + |z|$. Our argument shows that $x/11, y/11, z/11$ is also a solution, contradicting the choice of x, y, z).

Problem 9. a) Let $f(n) = n^2$ and $g(n) = \mu(n)n^2$. Show that $f * g = \delta$.
b) Let f, g be arithmetic functions with $n \mid f(n)$ and $n \mid g(n)$ for every n. Prove that $n \mid (f * g)(n)$ for every n.

Solution.

(a) We compute directly:

$$\begin{aligned}(f * g)(n) &= \sum_{d \mid n} f(d)\, g(n/d) = \sum_{d \mid n} d^2 \cdot \mu(n/d) \left(\frac{n}{d}\right)^2 \\ &= \sum_{d \mid n} d^2 \cdot \mu(n/d) \cdot \frac{n^2}{d^2} = n^2 \sum_{d \mid n} \mu(n/d) = n^2 \sum_{e \mid n} \mu(e).\end{aligned}$$

By the fundamental property of the Möbius function, $\displaystyle\sum_{e \mid n} \mu(e) = \delta(n)$, where $\delta(1) = 1$ and $\delta(n) = 0$ for $n > 1$. Therefore

$$(f * g)(n) = n^2 \cdot \delta(n) = \begin{cases} 1 & n = 1, \\ 0 & n > 1, \end{cases}$$

which is exactly $\delta(n)$. Hence $f * g = \delta$, i.e. $g = f^{-1}$ under Dirichlet convolution.

(b) Fix n. For each divisor $d \mid n$, we have $d \mid f(d)$ and $(n/d) \mid g(n/d)$, so

$$n = d \cdot \frac{n}{d} \mid f(d)\, g(n/d).$$

Hence $n \mid f(d)\, g(n/d)$ for each $d \mid n$. Thus each summand in the sum

$$(f * g)(n) = \sum_{d|n} f(d)\, g(n/d)$$

is divisible by n, so the sum is also divisible by n, i.e. $n \mid (f * g)(n)$, as required.