Solutions to Exam 2, Math 407 & Math 574

Problem 1. a) Explain the meaning of $[a_0, a_1, a_2, \ldots]$, where a_i are integers and $a_i > 0$ for $i = 1, 2 \ldots$. Given a real number x, how do we find integers $a_0, a_1, a_2, \ldots$ which are positive except possibly a_0 and such that $x = [a_0, a_1, a_2, , \ldots]$? (8 points)

b) Express $\sqrt{15}$ as a simple continued fraction. Explain carefully all details. (8 points)

c) What is the value of $[2, 3, 1, 3, 1, 3, 1, \ldots] = [2, \overline{3, 1}]$? Show all necessary work. (8 points)

d) Compute the fifth convergent of the continued fraction $x = [3, 1, 6, 1, 6, \ldots] = [3, \overline{1, 6}]$. Among all rational numbers whose denominator is at most 63, which one is closest to x? (8 points)

Solution. a) $[a_0, a_1, a_2, \ldots]$ is defined as the limit

$$[a_0, a_1, a_2, , \ldots] = \lim_{n\to\infty} [a_0, a_1, \ldots, a_n]$$

where

$$[a_0, a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}.$$

We proved that under the assumptions (a_i are integers and $a_i > 0$ for $i = 1, 2 \ldots$) the limit always exists and is an irrational number.

Given x, we define a sequence x_k recursively by $x_0 = x$ and $x_{k+1} = \dfrac{1}{x_k - \lfloor x_k \rfloor}$. When x is irrational this defines an infinite sequence. When x is rational, we get x_n to be an integer for some n and then we stop. We have $a_i = \lfloor x_i \rfloor$ for $i = 0, 1, \ldots$.

b) We start with $x_0 = \sqrt{15}$, $a_0 = \lfloor x_0 \rfloor = 3$. Thus

$$x_1 = \frac{1}{\sqrt{15} - 3} = \frac{3 + \sqrt{15}}{6} \quad \text{and} \quad \lfloor x_1 \rfloor = 1,$$

$$x_2 = \frac{1}{\frac{3+\sqrt{15}}{6} - 1} = \frac{6}{\sqrt{15} - 3} = \sqrt{15} + 3 \quad \text{and} \quad \lfloor x_2 \rfloor = 6,$$

$$x_3 = \frac{1}{(\sqrt{15} + 3) - 6} = \frac{1}{\sqrt{15} - 3} = x_1 \quad \text{and} \quad \lfloor x_3 \rfloor = 1.$$

At this point we see that $x_3 = x_1$, so $x_4 = x_2$, $x_5 = x_3 = x_1$, and so on. Thus

$$\sqrt{15} = [3, 1, 6, 1, 6, 1, 6 \ldots] = [3, \overline{1, 6}].$$

c) We have $[2, \overline{3, 1}] = 2 + \dfrac{1}{[\overline{3, 1}]}$. So we first compute the purely periodic part $x = [\overline{3, 1}]$:

$$x = 3 + \cfrac{1}{1 + \cfrac{1}{x}} = 3 + \frac{x}{x + 1} = \frac{4x + 3}{x + 1}.$$

Thus $x^2+x=4x+3$ and $x^2-3x-3=0$. It follows that $x=\frac{3\pm\sqrt{21}}{2}$. Since $x\geq 2$, we have $x=\frac{3+\sqrt{21}}{2}$. Thus

$$[2,\overline{3,1}]=[2,x]=2+\frac{1}{x}=2+\frac{2}{3+\sqrt{21}}=2+\frac{2(\sqrt{21}-3)}{21-9}=2+\frac{\sqrt{21}-3}{6}=\frac{\sqrt{21}+9}{6}.$$

c) The k-the convergent of a continued fraction $[a_0,a_1,a_2,\ldots]$ is $[a_0,a_1,\ldots,a_k]=\frac{p_k}{q_k}$, where the numbers p_i, q_i are defined recursively by

$$p_n=a_np_{n-1}+p_{n-2}, p_{-1}=1, p_0=a_0, \quad \text{and} \quad q_n=a_nq_{n-1}+q_{n-2}, q_{-1}=0, q_0=1.$$

Alternatively, we can use the formula

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix}\cdots\begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}=\begin{bmatrix} p_k \\ q_k \end{bmatrix}.$$

In our case, $x=[3,1,6,1,6,1,\ldots]$. Thus

$$p_0=3, p_1=4, p_2=27, p_3=31, p_4=213, p_5=244$$

and

$$q_0=1, q_1=1, q_2=7, q_3=8, q_4=55, q_5=63.$$

Thus the fifth convergent for x is $\frac{244}{63}$.

We proved that among all fractions with denominator bounded by q_k, the closed to x is the k-th convergent. Thus among all fractions whose denominator does not exceed 63, the closest to x is $\frac{244}{63}$.

Problem 2. a) Define the Legendre symbol and the Jacobi symbol. State quadratic reciprocity. (8 points)

b) Is the congruence $x^2+10x+7\equiv 0 \pmod{2017}$ solvable? Carefully justify your answer. You can use the fact that 2017 is a prime. (8 points)

c) Find all solutions to the congruence $3x^2-2x-9\equiv 0 \pmod{19}$. (8 points)

Solution. a) An integer a is called a **quadratic residue** modulo a prime p if $p\nmid a$ and $a\equiv x^2 \pmod{p}$ for some integer x. An integer a is called a **quadratic non-residue** modulo a prime p if there is no integer x such that $a\equiv x^2 \pmod{p}$. When p is an odd prime then we define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows

$$\left(\frac{a}{p}\right)=\begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p; \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p; \\ 0 & \text{if } p|a. \end{cases}$$

The Jacobi symbol $\left(\frac{a}{m}\right)$ is defined for any integer a and any odd integer m as follows: write $m=p_1\ldots p_s$ as a product of prime numbers and set

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right).$$

Qadratic Reciprocity:

1. If p and q are distinct odd prime numbers then

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \equiv q \pmod 4 \ ; \\ \left(\frac{p}{q}\right) & \text{if at least one of } p, q \text{ is} \equiv 1 \pmod 4 \ . \end{cases}$$

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

2. $$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \ ; \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \ . \end{cases}$$

Equivalently, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

3. $$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \ ; \\ -1 & \text{if } p \equiv 3 \pmod 4 \ . \end{cases}$$

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

Remark. Often by quadratic reciprocity one only means part 1. The other two parts are simpler and were proved earlier.

Qadratic Reciprocity for Jacobi symbol:

1. If m and n are distinct odd numbers then

$$\left(\frac{n}{m}\right) = \begin{cases} -\left(\frac{m}{n}\right) & \text{if } m \equiv 3 \equiv n \pmod 4 \ ; \\ \left(\frac{m}{n}\right) & \text{if at least one of } m, n \text{ is} \equiv 1 \pmod 4 \ . \end{cases}$$

Equivalently, if m, n are relatively prime, then $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

2. $$\left(\frac{2}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1, 7 \pmod 8 \ ; \\ -1 & \text{if } m \equiv 3, 5 \pmod 8 \ . \end{cases}$$

Equivalently, $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

3. $$\left(\frac{-1}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1 \pmod 4 \ ; \\ -1 & \text{if } m \equiv 3 \pmod 4 \ . \end{cases}$$

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

b) Note that $x^2 + 10x + 7 = (x+5)^2 - 18$. Thus our congruence is equivalent to $(x+5)^2 \equiv 18 \pmod{2017}$. This congruence is solvable if and only if 18 is a square modulo 2017. We have

$$\left(\frac{18}{2017}\right) = \left(\frac{2}{2017}\right)\left(\frac{9}{2017}\right) = \left(\frac{2}{2017}\right) = 1$$

since $2017 \equiv 1 \pmod 8$. Thus 18 is indeed a square modulo 2017 and our congruence is solvable

Remark. In general, if p is an odd prime and $p \nmid a$ then a quadratic congruence $ax^2 + bx + c \equiv 0 \pmod p$ is solvable if and only if the discriminant $b^2 - 4ac$ is a square modulo p.

c) The congruence $3x^2 - 2x - 9 \equiv 0 \pmod{19}$ is equivalent to $3(3x^2 - 2x - 9) \equiv 0 \pmod{19}$, which is the same as $(3x-1)^2 \equiv 28 \equiv 9 = 3^2 \pmod{19}$. It follows that

$3x - 1 \equiv 3 \pmod{19}$ or $3x - 1 \equiv -3 \pmod{19}$. The first congruence has solution $x \equiv 14 \pmod{19}$, the second congruence has solution $x \equiv 12 \pmod{19}$.

Problem 3. a) Define perfect numbers. What can you say about even perfect numbers? (7 points)

b) Prove that if $k > 1, m > 1$ are integers then $\sigma(km) > k\sigma(m)$. (7 points)

c) Show that if m, n are perfect numbers and $m|n$ then $m = n$. (7 points)

Solution. a) A positive integer n is called **perfect** if it is equal to the sum of all its proper divisors, i.e. if $\sigma(n) = 2n$, where $\sigma(n)$ is the sum of all positive divisors of n. It was proved by Euclid and Euler that an even number n is perfect if and only if $n = 2^{k-1}(2^k - 1)$ for some k such that $2^k - 1$ is a prime number. It is not known if there exists an odd perfect number.

b) Let $d_1, d_2, \ldots, d_s$ be all the positive divisors of m, so $\sigma(m) = d_1 + \ldots + d_s$. Each of the numbers $1, kd_1, kd_2, \ldots, kd_s$ is a positive divisor of km. Thus

$$\sigma(km) \geq 1 + kd_1 + kd_2 + \ldots + kd_s = 1 + k\sigma(m) > k\sigma(m).$$

c) Suppose that m is a perfect number and $n = km$ for $k > 1$. Then $\sigma(m) = 2m$ and, by part b), we have

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

so $sigma(n) > 2n$, i.e. n is not perfect.

Problem 4. a) Define the Möbius function. State the Möbius inversion formula. (8 points)

b) Let $f(n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even.} \end{cases}$ Show that f is multiplicative. (7 points)

c) Let $g = \phi * f$ (here ϕ is the Euler function). Prove that $g(n) = \begin{cases} n & \text{if } n \text{ is odd} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$ (8 points)

Solution. a) The Möbius function μ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 p_2 \ldots p_r \text{ is a product of } r \text{ distinct primes,} \\ 0 & \text{in all other cases.} \end{cases}$$

It is the convolution inverse of $\mathbb{1}$.

Möbius inversion formula: if $F = f * \mathbb{1}$ then $f = F * \mu$. In other words, if $F(n) = \sum_{d|n} f(d)$ for all n, then $f(n) = \sum_{d|n} F(d)\mu(n/d)$ for all n.

b) We will show that f is completely multiplicative. If at least one of m, n is even then $f(m)f(n) = 0$ an mn is also even, so $0 = f(mn)$. Thus $f(mn) = f(m)f(n)$ in this case. If both m and n are odd then $f(m) = 1 = f(n)$ and mn is also odd. Thus $1 = f(mn) = f(m)f(n)$.

c) Since f and ϕ are both multiplicative, so is $\phi * f$. If $k \geq 1$ then

$$(\phi * f)(2^k) = \sum_{i=0}^{k} \phi(2^i)f(2^{k-i}) = \phi(2^k) = 2^{k-1}$$

since $f(2^{k-i}) = 0$ for $i < k$. When m is odd then so is every divisor of m so

$$(\phi * f)(m) = \sum_{d|m} \phi(d)f(m/d) = \sum_{d|m} \phi(d) = m$$

since we proved that $\sum_{d|n} \phi(d) = n$ for every n (alternatively, compute $(\phi * f)(p^k)$ of powers of odd primes p and use multiplicativity). This, if n is odd we have $(\phi * f)(n) = n$ and if $n = 2^k m$ is even, with $k > 0$ and m odd we have

$$(\phi * f)(n) = (\phi * f)(2^k m) = (\phi * f)(2^k)(\phi * f)(m) = 2^{k-1}m = n/2.$$

Problem 5. Suppose that $x = [a_0, a_1, a_2, \ldots, a_n]$ and $a_1 > 1$. Show that

$$-x = [-a_0 - 1, 1, a_1 - 1, a_2, a_3, \ldots, a_n].$$

What if $a_1 = 1$?

Solution. Let $z = [a_2, a_3, \ldots, a_n]$. Then $x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{z}}$ and

$$[-a_0 - 1, 1, a_1 - 1, a_2, a_3, \ldots, a_n] = -a_0 - 1 + \cfrac{1}{1 + \cfrac{1}{a_1 - 1 + \cfrac{1}{z}}} = -a_0 - 1 + \frac{a_1 - 1 + \frac{1}{z}}{a_1 + \frac{1}{z}} =$$

$$= -a_0 - \cfrac{1}{a_1 + \cfrac{1}{z}} = -x.$$

This computation works when $n \geq 2$, but when $n = 1$ we can replace $1/z$ with 0 and it still works.

When $a_1 = 1$, the above does not work as $a_1 - 1 = 0$ is not allowed in a continued fraction. We have $-[a_0, 1, a_2, \ldots, a_n] = [-a_0 - 1, 1 + a_2, a_3, \ldots, a_n]$.