Quizzes for Math 407

QUIZ 1. a) State the division algorithm.

b) Use Euclid's algorithm to compute $\gcd(803, 154)$ and find integers m, n such that $\gcd(803, 154) = m \cdot 803 + n \cdot 154$.

Solution: a) **Theorem (Division Algorithm):** Let a, b be integers such that $a \neq 0$. Then there exist integers k, r such that

$$b = ka + r \quad \text{and} \quad 0 \leq r < |a|.$$

Both k and r are unique. When $a > 0$, the long division algorithm produces k and r.

b) We run Euclid's algorithm with $a_0 = 803$ and $a_1 = 154$:

$$a_0 = 803 = 5 \cdot 154 + 33 = 5a_1 + 33; \ a_2 = 33$$

$$a_1 = 154 = 4 \cdot 33 + 22 = 4a_2 + 22; \ a_3 = 22$$

$$a_2 = 33 = 1 \cdot 22 + 11 = 1 \cdot a_3 + 11; \ a_4 = 11$$

$$a_3 = 22 = 2 \cdot 11 + 0 = 2a_4 + 0; \ a_5 = 0$$

Thus $\gcd(803, 154) = a_4 = 11$.

We can now work "backwards" to find

$$11 = 33 - 22 = 33 - (154 - 4 \cdot 33) = 5 \cdot 33 - 154 = 5(803 - 5 \cdot 154) - 154 = 5 \cdot 803 - 26 \cdot 154.$$

so $m = 5$, $n = -26$ work.

Alternatively, we can use the matrix interpretation of the algorithm, which yields:

$$\begin{pmatrix}11\\0\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -4\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -5\end{pmatrix}\begin{pmatrix}803\\154\end{pmatrix}.$$

Multiplying the matrices, we get

$$\begin{pmatrix}11\\0\end{pmatrix} = \begin{pmatrix}5 & -26\\-14 & 73\end{pmatrix}\begin{pmatrix}803\\154\end{pmatrix}.$$

It follows that $11 = 5 \cdot 803 - 26 \cdot 154$, so $m = 5$, $n = -26$ work.

QUIZ 2. a) State Euclid's Lemma.

b) Define Fermat's primes.

c) Let n be an integer. Prove that $\gcd(3n+1, 5n+2) = 1$.

Solution: a) **Euclid's Lemma.** If p is a prime number and m, n are integers such that $p|mn$ then either $p|m$ or $p|n$.

b) Fermat's primes are prime numbers of the form $2^{2^n}+1$ for some prime n. The only known Fermat's primes are those corresponding to $n = 0, 1, 2, 3, 4$. It is an open problem whether there are other Fermat's primes.

c) Let $d = \gcd(3n+1, 5n+2)$. Then d divides $3n+1$ and $5n+2$. Thus d divides $a(3n+1)+b(5n+2)$ for any integers a, b. Take $a = -5$, $b = 3$. We see that d divides the number

$$-5(3n+1) + 3(5n+2) = 1.$$

It follows that $d = 1$.

QUIZ 3.a) Define the inverse of an integer a modulo m. When does a have the inverse?

b) Find the inverse of 23 modulo 67.

c) Find all solutions to the congruence $9x \equiv 6(\mod 12)$.

Solution: a) An inverse of a modulo m is any integer b such that $ab \equiv 1(\mod m)$. It exists if and only if $\gcd(a, m) = 1$. When it exists, it is unique modulo m.

b) We use the Euclidean algorithm:

$$67 = 2 \cdot 23 + 21, \quad 23 = 1 \cdot 21 + 2, \quad 21 = 10 \cdot 2 + 1, \quad 2 = 2 \cdot 1 + 0.$$

It follows that

$$1 = 21 - 10 \cdot 2 = 21 - 10(23 - 21) = 11 \cdot 21 - 10 \cdot 23 = 11(67 - 2 \cdot 23) - 10 \cdot 23 = -32 \cdot 23 + 11 \cdot 67.$$

Thus $-32 \cdot 23 \equiv 1 (\mod 67)$. As $-32 \equiv 35 (\mod 67)$, 35 is the inverse of 23 modulo 67.

c) Clearly $\gcd(9, 12) = 3$. Since $3|6$, the congrunce will have 3 solutions modulo 12. It is easy to see that $x = 2$ is a solution. Thius the solutions are 2, $2 + 4 = 6$, and $2 + 2 \cdot 4 = 10$. For a detailed discussion of the method see solution to Problem 28e) from homework 3.

QUIZ 4. a) State the Chinese Remainder Theorem.

b) State Euler's theorem and define the Euler's function ϕ.

c) Find the reminder of 3^{337} modulo 31.

Solution. a) **Chinese Remainder Theorem:** Let $n_1, ..., n_k$ be pairwise relatively prime positive integers and let $N = n_1 \cdot n_2 \cdot ... \cdot n_k$. Given any integers $a_1, ..., a_k$, the system of congruences

$$x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, \ldots, x \equiv a_k \pmod{n_k}$$

has unique solution x such that $0 \leq x < N$. Moreover, an integer y satisfies these congruences iff $N|(x - y)$ (so all integers satisfying the congruences are given by $x + mN$, $m \in \mathbb{Z}$).

b) **Euler's Theorem:** Let n be a positive integer. Then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for any integer a relatively prime to n.

Euler's function ϕ assigns to each positive integer n the number $\phi(n)$ of positive integers which are relatively prime to n and smaller or equal than n. In other words,

$\phi(n)$ is the number of elements in the set

$$U_n = \{k : 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}.$$

Equivalently, $\phi(n)$ is the number of invertible elements in $\mathbb{Z}/n\mathbb{Z}$ (for $n > 1$).

c) By Fermat's Little theorem we have $3^{30} \equiv 1 \pmod{31}$. Note that $337 = 30 \cdot 11 + 7$, so

$$3^{337} = 3^{30 \cdot 11 + 7} = (3^{30})^{11} \cdot 3^7 \equiv 1^{11} \cdot 3^7 = 3^7 \pmod{31} .$$

Now $3^3 = 27 \equiv -4 \pmod{31}$ and $3^4 = 3 \cdot 3^3 \equiv 3 \cdot (-4) = -12 \pmod{31}$. Thus $3^7 = 3^3 \cdot 3^4 \equiv (-4)(-12) = 48 \equiv 17 \pmod{31}$. Therefore $3^{337} \equiv 17 \pmod{31}$.

QUIZ 5. a) State Wilson's Theorem.

b) Let $m > 1$ be an integer. Explain how exponent of m is defined.

c) Let $a > 1$ be an integer and let $m = a^2 + 1$. Explain why $\text{ord}_m a = 4$.

Solution. a) **Wilson's Theorem**. A positive integer p is a prime number if and only if $(p-1)! \equiv -1 \pmod{p}$.

b) The **exponent of** m is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$ for every integer a relatively prime to m.

c) Note that $a^4 - 1 = (a^2 + 1)(a^2 - 1) = m(a^2 - 1)$, so m divides $a^4 - 1$, i.e. $a^4 \equiv 1 \pmod{m}$. This means that the order $\text{ord}_m a$ divides 4. Thus the order is one of the numbers $1, 2, 4$. The order is not 1 as $a - 1$ is not divisible by m (since $0 < a - 1 < m$). If the order was 2 we would have $m | a^2 - 1$, which is not possible since $0 < a^2 - 1 < a^2 + 1$. Thus the order $\text{ord}_m a = 4$.

QUIZ 6. a) For which of the following values of m a primitive root modulo m exists: 14, 24, 30, 54? Explain your answer by quoting a result.

b) Find the smallest $k > 0$ such that $a^k \equiv 1 \pmod{72}$ for every integer a relatively prime to 72.

c) a is a primitive root modulo 17. What is $\text{ord}_{17} a^{12}$? What is $a^8 \pmod{17}$?

Solutions. a) To answer the question we use the primitive root theorem.

Primitive Root Theorem. Let $m > 1$ be an integer. A primitive root modulo m exists if and only if m is one of the numbers on the following list: $2, 4, p^a, 2p^a$, where p is an odd prime and a is a positive integer.

Now $14 = 2 \cdot 7$ and $54 = 2 \cdot 3^3$ are on the above list so a primitive root modulo 14 or modulo 54 exist. On the other hand $24 = 2^3 \cdot 3$ and $30 = 2 \cdot 3 \cdot 6$ are not on the list, so primitive roots modulo 24 and modulo 30 do not exist.

b) Recall the exponent theorem.

Exponent Theorem. Let $m = 2^a p_1^{a_1} \dots p_s^{a_s}$, where $p_1 < p_2 < \dots < p_s$ are odd prime numbers. The smallest $k > 0$ such that $a^k \equiv 1 \pmod{m}$ for every integer a relatively prime to m, called the exponenet of m, is given by the following formula:

$$\text{exponent}(m) = \text{lcm}(\text{exponent}(2^a), \phi(p_1^{a_1}), \dots, \phi(p_s^{a_s})).$$

Recall also that

$$\text{exponent}(2^a) = \begin{cases} 1 & \text{if } a = 0 \text{ or } a = 1 \\ 2 & \text{if } a = 2 \\ 2^{a-2} & \text{if } a \geq 3 \end{cases}$$

Since $72 = 2^3 \cdot 3^2$, we have

$$\text{exponent}(72) = \text{lcm}(\text{exponent}(2^3), \phi(3^2)) = \text{lcm}(2, 6) = 6.$$

c) Since a is a primitive root modulo 17, we have $\text{ord}_{17} a = \phi(17) = 16$. We us the following general formula:

$$\text{ord}_m a^k = \frac{\text{ord}_m a}{\gcd(k, \text{ord}_m a)}.$$

Thus

$$\text{ord}_{17} a^{12} = \frac{\text{ord}_{17} a}{\gcd(12, \text{ord}_{17} a)} = \frac{16}{\gcd(12, 16)} = 4.$$

Since $\text{ord}_{17} a = 16$, we have $a^8 \not\equiv 1 \pmod{17}$ and $a^{16} = (a^8)^2 \equiv 1 \pmod{17}$. Since ± 1 are the only solutions of the congruence $x^2 \equiv 1 \pmod{p}$ for any prime p, we see that $a^8 \equiv -1 \pmod{17}$.

QUIZ 7. a) What is the length of the (shortest) period in the decimal expansion of $\frac{57}{9999}$? Is the expansion purely periodic?

b) What does it mean that a is an n-th power residue modulo m?

c) Is the congruence $x^4 \equiv -13 \pmod{34}$ solvable?

Solutions. a) Let us recall some results from class. Consider a fraction a/b, where $1 \leq a < b$ and $\gcd(a, b) = 1$. Write $b = 2^u 5^w B$, where $\gcd(B, 10) = 1$. Then:

1. the decimal expansion of a/b is finite if and only if $B = 1$.
2. if $B > 1$ then the decimal expansion of a/b is periodic with (shortest) period of length $s = \mathrm{ord}_B 10$. The decimal expansion is of the form

$$0.a_1 a_2 \ldots a_k \overline{b_1 b_2 \ldots b_s},$$

where $b_1, \ldots, b_s, a_1, \ldots, a_k$ are digits, $b_s \neq a_k$, and $k = \max(u, w)$. In particular, the expansion is purely periodic if and only if $u = w = 0$.

One way to find the integers $\alpha = a_1 10^{k-1} + a_2 10^{k-2} + \ldots + a_k$ and $\beta = b_1 10^{s-1} + b_2 10^{s-2} + \ldots + b_s$ is as follows: first find $s = \mathrm{ord}_B 10$ and set $k = \max(u, w)$. Then use the division algorithm to get

$$2^{k-u} 5^{k-w} a = pB + q, \ 1 \leq q < B.$$

Then $\alpha = p$ and $\beta = q(10^s - 1)/B$.

Another way is to perform long division $a : b$ untill the process starts repeating. Then you can read the values of α, β, s, k from the long division.

We are ready now to solve part a). Note that $\gcd(57, 9999) = 3$. Thus $57/9999 = 19/3333$ and $\gcd(19, 3333) = 1$ We have $a = 19$, $b = 3333 = (10^4 - 1)/3$, $B = b$, $u = w = k = 0$. The length of the period is $\mathrm{ord}_{3333} 10 = 4$ (clearly $3333 | 10^4 - 1$ and $3333 > 10^3 - 1$ so 4 is the smallest positive integer m such that $10^m - 1$ is divisible by 3333). The expansion is purely periodic since $k = 0$.

b) a is an n-th power residue modulo m if $\gcd(a, m) = 1$ and the congruence $x^n \equiv a \pmod{m}$ is solvable.

c) Let us recall the following result from class.

Theorem. Let $m > 1$, $n > 0$, a be integers.

(i) If a is n-th power residue modulo m then

$$a^{\phi(m)/\gcd(n,\phi(m))} \equiv 1 \pmod{m} .$$

(ii) if a primitive root modulo m exists and

$$a^{\phi(m)/\gcd(n,\phi(m))} \equiv 1 \pmod{m}$$

then a is n-th power residue modulo m.

Part c) asks if the congruence $x^4 \equiv -13 \pmod{34}$ solvable, i.e. if -13 is a 4-th power residue modulo 34 (we usually say *quartic residue*). Since $34 = 2 \cdot 17$, a primitive root modulo 34 exists. Thus -13 is a 4-th power residue modulo 34 if and only if

$$(-13)^{\phi(34)/\gcd(4,\phi(34))} = (-13)^4 \equiv 1 \pmod{34} .$$

Since $(-13)^4 \equiv 1 \pmod{2}$, it suffices to verify whether $(-13)^4 \equiv 1 \pmod{17}$. Now $-13 \equiv 4 \pmod{17}$ so

$$(-13)^4 \equiv 4^4 = (16)^2 \equiv (-1)^2 = 1 \pmod{17} .$$

Thus the answer is yes, -13 is a 4-th power residue modulo 34.

QUIZ 8. a) State Euler's criterion.

b) Define the Legendre's symbol $\left(\frac{a}{p}\right)$.

c) Is 2 a quadratic residue modulo 97? Explain your answer.

Solution. a) **Euler's Criterion.** An integer a is a quadratic residue modulo a prime p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. Equivalently, $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

b) 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

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

c) We use the following theorem: if p is an odd prime number then

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

Since 97 is a prime, we have

$$\left(\frac{2}{97}\right) = (-1)^{\frac{97^2-1}{8}} = (-1)^{12\cdot 98} = 1.$$

Thus 2 is a quadratic residue modulo 97.

QUIZ 9. a) Is the congruence $x^2 + 5x - 9 \equiv 0 \pmod{59}$ solvable?

b) Express $13 \cdot 17$ as a sum of two squares of integers.

c) Fing a right triangle whose side-lengths are integers and whose hypotenuse has length 29.

Solution. a) A quadratic congruence $ax^2 + bx + x \equiv 0 \pmod{p}$, where $p \nmid a$, p a prime, is solvable if and only if the discriminant $b^2 - 4ac$ is a square modulo p (see the solution to problem 10 from homework 8 for more details). In our case $a = 1, b = 5, c = -9$ so the discriminant is $25 + 36 = 61$. Since

$$\left(\frac{61}{59}\right) = \left(\frac{2}{59}\right) = -1$$

(since $59 \equiv 3 \pmod{8}$), the congruence has no solutions.

One can also solve the problem by completing to squares: note that $5 \equiv -54 \pmod{59}$, so

$$x^2 + 5x - 9 \equiv x^2 - 54 - 9 = x^2 - 2 \cdot 27 + 27^2 - 27^2 - 9 \equiv (x - 27)^2 - 30 \pmod{59}.$$

Thus the congruence is solvable if and only if 30 is a quadratic residue modulo 59. Now

$$\left(\frac{30}{59}\right) = \left(\frac{2^2}{59}\right)\left(\frac{30}{59}\right) = \left(\frac{120}{59}\right) = \left(\frac{2}{59}\right) = -1$$

(we used a trick here to speed up the computation).

b) We have $13 = 3^2 + 2^2$ and $17 = 4^2 + 1^2$. Thus

$$13 \cdot 17 = (3^2 + 2^2)(4^2 + 1^2) = (3 \cdot 4 \mp 2 \cdot 1)^2 + (3 \cdot 1 \pm 2 \cdot 4)^2 = 10^2 + 11^2 = 14^2 + 5^2.$$

c) Recall that primitive Pythagorean triples (a, b, c) with b even are generated by the formulas $a = m^2 - n^2, b = 2mn$, $c = m^2 + n^2$, for some relatively prime integers m, n of different parity.

We have $29 = 5^2 + 2^2$. Taking $a = 5^2 - 2^2 = 21$, $b = 2 \cdot 5 \cdot 4 = 20$ we see that the triangle with sides of length $20, 21, 29$ is right.

QUIZ 10. a) What is $\phi * \nu(12)$, where ϕ is the Euler function and ν is the number of divisors function.

b) The arithmetic function f is multiplicative and satisfies the condition

$$0 \leq f(p^k) \leq k + 1$$

for every prime p and every non-negative integers k. Prove that $f(n) \leq \nu(n)$ for all n.

c) Prove that there are no integers X, Y such that $X^3 + 6Y^3 = 4$. Hint: work modulo an appropriate prime.

Solution. a) Let us start by reviewing some basis properties of convolution.

Let R be a commutative ring (main examples are $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$). An arithemtic R-valued function is a function $f : \mathbb{N} \longrightarrow R$. By $\mathcal{A}(\mathcal{R})$ we denote the set of all arithmetic R-valued functions. For $f, g \in \mathcal{A}(\mathcal{R})$ we define $f + g$ by
$(f + g)(n) = f(n) + g(n)$ for all positive integers n. The function $f - g$ is defined by $(f - g)(n) = f(n) - g(n)$.

For $f, g \in \mathcal{A}(\mathcal{R})$ we define the **convolution** $f * g$ as follows:

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

for any positive integer n, The convolution has the following properties:

1. it is commutative: $f * g = g * f$.
2. it is associative: $(f * g) * h = f * (g * h)$.
3. it disctibutes over addition: $(f + g) * h = f * h + g * h$.
4. the function δ defined by

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

   is the identity element for convolution: $f * \delta = f$ for any f.
5. f is invertible under convolution (i.e. there exists g such that $f * g = \delta$) if and only if $f(1)$ is invertible in R. In particular, all non-zero multiplicative functions are invertible under convolution (as $f(1) = 1$ if f is mutiplicative).
6. if any two of the three functions f, g, $f * g$ are multiplicatiove then so is the third; in particular, the convolution of two multiplicative functions is multiplicative and the convolution inverse of a multiplicative function f is multiplicative, i.e. if $f * g = \delta$ then g is multiplicative.
7. if R is an integral domain (i.e. for any $a, b \in R$ such that $ab = 0$ we have $a = 0$ or $b = 0$), then $\mathcal{A}(\mathcal{R})$ is an integral domain, i.e. if $f * g = 0$ then $f = 0$ or $g = 0$.
8. define $\mathbb{1}$ to be the constatnt function 1, i.e. $\mathbb{1}(n) = 1$ for all n. Clearly $\mathbb{1}$ is multiplicative. The convolution inverse of $\mathbb{1}$ is called the Möbius function and it is denoted bt μ. We have

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

9. 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.

We can now solve part a). We can use the definition of convolution:

$$\phi * \nu(12) = \phi(1)\nu(12) + \phi(2)\nu(6) + \phi(3)\nu(4) + \phi(4)\nu(3) + \phi(6)\nu(2) + \phi(12)\nu(1) =$$

$$1 \cdot 6 + 1 \cdot 4 + 2 \cdot 3 + 2 \cdot 2 + 2 \cdot 2 + 4 \cdot 1 = 28.$$

Alternatively, we can observe that $\phi * \nu$ is multiplicative, so $\phi * \nu(12) = \phi * \nu(3) \cdot \phi * \nu(4) = 4 \cdot 7 = 28$, since $\phi * \nu(3) = 4$ and $\phi * \nu(4) = 7$ (which is computed as in the first solution)

b) Note that $\nu(p^k) = k+1$ for every prime p and every non-negative integers k. Thus we are given that $0 \leq f(p^k) \leq \nu(p^k)$ every prime p and every non-negative integers k. If n is a positive integer, we can factor n into product of powers of disctinct primes $n = p_1^{k_1} \dots p_s^{k_s}$ and use the multiplicativity of f and ν to get

$$f(n) = f(p_1^{k_1}) \dots f(p_s^{k_s}) \leq \nu(p_1^{k_1}) \dots \nu(p_s^{k_s}) = \nu(n).$$

c) We work modulo 7. The key observation is that a cube of any integer is congruent to one of $0, 1$, or -1 modulo 7. Indeed, if $7|a$ then $a^3 \equiv 0 \pmod 7$ and if $7 \nmid a$ then $a^6 = (a^3)^2 \equiv 1 \pmod 7$ (by Fermat's Little Theorem), so $a^3 \equiv \pm 1 \pmod 7$. Note that $X^3 + 6Y^3 \equiv X^3 - Y^3 \pmod 7$ and the the possible values of $a - b$, where both a, b are in $\{-1, 0, 1\}$ are $-2, -1, 0, 1, 2$, none of which is congruent to 4 mod 7. Thus the congruence $X^3 + 6Y^3 \equiv 4 \pmod 7$ has no solutions, and therefore there are no integers X, Y such that $X^3 + 6Y^3 = 4$.

Second method. Another way to solve part c) is to study divisibility by powers of 2. Note that if $X^3 + 6Y^3 = 4$ then X^3 must be even. This means that $8|X^3$ and therefore $8|(4 - 6Y^3)$. This implies that $4|6Y^3$ and therefore $2|Y^3$. However this means that Y is even and therefore $8|Y^3$. We see that 8 divides X^3 and Y^3, so it divides $X^3 + 6Y^3 = 4$, which is clearly not possible.

QUIZ 11. a) Express $\dfrac{43}{30}$ as a finite simple continued fraction.

b) What is the value of $[2,1,1,2,1,1,2,1,1,\ldots]$?

c) Which is bigger: $[2,1,3,4,7,2]$ or $[2,1,3,5,7,1]$? Hint: Do not evaluate these expressions. Think. Note that $[2,1,3,[4,7,2]]$. What can you say about $[4,7,2]$ and $[5,7,1]$?

Solution. a) We apply Euclidean algorithm to 43 and 30:

$$43 = 1 \cdot 30 + 13, \quad 30 = 2 \cdot 13 + 4, \quad 13 = 3 \cdot 4 + 1, \quad 4 = 4 \cdot 1 + 0.$$

It follows that

$$\frac{43}{30} = [1,2,3,4] = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4}}}.$$

b) Let $x = [2,1,1,2,1,1,2,1,1,\ldots]$, so $x = [2,1,1,x]$. In other words,

$$x = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{x}}} = 2 + \cfrac{1}{1 + \cfrac{x}{x+1}} = 2 + \frac{x+1}{2x+1} = \frac{5x+3}{2x+1}.$$

Thus $x(2x+1) = 5x+3$, i.e. $2x^2 - 4x - 3 = 0$. The solutions to this quadratic equation are $(2 \pm \sqrt{10})/2$. Since $x > 2$, we have $x = (2+\sqrt{10})/2$.

c) First recall that if two simple continued fractions x=$[k_0, k_1, \ldots, k_s]$ and y=$[l_0, l_1, \ldots, l_t]$ are not equal and $k_0 < l_0$ then $x < y$ (since $x \le k_0 + 1 \le l_0 \le y$). Also recall that two simple continued fractions x=$[k_0, k_1, \ldots, k_s]$ and y=$[l_0, l_1, \ldots, l_t]$ with $s \le t$ are equal if and only if either they are the same or $t = s+1$, $l_i = k_i$ for $i = 0, \ldots, s-1$, $l_s = k_s - 1$ and $l_{s+1} = 1$.

We see that $[4,7,2] < [5,7,1]$.

Finally recall that if m is even then $[k_0, k_1, \ldots, k_m, x]$ is a decreasing function of x and if m is odd then $[k_0, k_1, \ldots, k_m, x]$ is an increasing function of x.

Thus $[2,1,3,x]$ is a decreasing function of x ($m = 2$). Since $[4,7,2] < [5,7,1]$ we have $[2,1,3,[4,7,2]] > [2,1,3,[5,7,1]]$, i.e. $[2,1,3,4,7,2] > [2,1,3,5,7,1]$.

Same method gives the following general result. Suppose that $[k_0, k_1, \ldots, k_s]$ and $[l_0, l_1, \ldots, l_t]$ are two finite simple continued fractions which **are not equal**. Suppose there exist i such that $k_i \neq l_i$ and let r be the smallest such i. Say $k_r > l_r$. Then

$$[k_0, k_1, \ldots, k_s] > [l_0, l_1, \ldots, l_t] \text{ if } r \text{ is even}$$

and

$$[k_0, k_1, \ldots, k_s] < [l_0, l_1, \ldots, l_t] \text{ if } r \text{ is odd.}$$

This also applies to infinite continued fractions.

QUIZ 12. a) What is the meaning of an infinite simple continued fraction $[k_0, k_1, k_2, \ldots]$?

b) When does a real number x have a periodic simple continued fraction represenattion?

c) Express $\sqrt{3}/2$ as simple countinued fraction.

Solution. a) An infinite simple continued fraction is defined as

$$[k_0, k_1, k_2, \ldots] = \lim_{n\to\infty} [k_0, k_1, \ldots, k_n]$$

where $k_0, k_1, \ldots$ is an infinite sequence of integers such that $k_1, k_2, \ldots$ are positive. We proved that the limit always exists and it is an irrational number. The s-th convergent of $[k_0, k_1, k_2, \ldots]$ is the value of the finite continued fraction $[k_0, k_1, \ldots, k_s]$, $s = 0, 1, \ldots$.

b) A real number x has a periodic simple continued fraction represenattion if and only if x is an irrational number of the form $(a + \sqrt{d})/b$ for some integers a, b, d (for x to be irrational is equivalent that d is not a square). Equivalently, x satisfies $Ax^2 + Bx + C = 0$ for some integers A, B, C such that $B^2 - 4AC > 0$ is not a square.

c) Recall that if $\alpha_0 = \sqrt{3}/2$, $\alpha_{n+1} = \dfrac{1}{\alpha_n - \lfloor \alpha_n \rfloor}$ and $k_n = \lfloor \alpha_n \rfloor$ then $\sqrt{3}/2 = [k_0, k_1, \ldots]$. We have $k_0 = \lfloor \alpha_0 \rfloor = 0$,

$$\alpha_1 = \frac{1}{\sqrt{3}/2} = \frac{2\sqrt{3}}{3}, \quad k_1 = \lfloor \alpha_1 \rfloor = 1, \quad \alpha_2 = \frac{1}{\frac{2\sqrt{3}}{3} - 1} = \frac{3}{2\sqrt{3} - 3} = 2\sqrt{3} + 3,$$

$$k_2 = \lfloor \alpha_2 \rfloor = 6, \alpha_3 = \frac{1}{2\sqrt{3} + 3 - 6} = \frac{3 + 2\sqrt{3}}{3}, k_3 = \lfloor \alpha_3 \rfloor = 2, \alpha_4 = \frac{1}{\frac{3+2\sqrt{3}}{3} - 2} =$$

$$\frac{3}{2\sqrt{3}-3} = 3 + 2\sqrt{3} = \alpha_2.$$

We see that $\alpha_2 = \alpha_4$. It follows that

$$\sqrt{3}/2 = [0, 1, 6, 2, 6, 2, \ldots] = [0, 1, \overline{6, 2}].$$