Quizzes for Elementary Number Theory

QUIZ 1. Use Euclid's algorithm to compute $\gcd(803, 154)$ and find integers λ, μ such that $\gcd(803, 154) = \lambda \cdot 803 + \mu \cdot 154$. Show all your work.

Solution: Let us recall Euclid's algorithm. To find $\gcd(a, b)$ set $a_1 = a$, $b_1 = b$ and apply the following procedure: given a_n, b_n, if $b_n = 0$ then stop: $a_n = \gcd(a, b)$. Otherwise, use division algorithm to write $a_n = k_n b_n + r_n$ with $0 \leq r_n < |b_n|$, set $a_{n+1} = b_n$, $b_{n+1} = r_n$, and repeat the procedure. It is easy to see that for any m

$$\begin{pmatrix} a_{m+1} \\ b_{m+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -k_m \end{pmatrix} \begin{pmatrix} a_m \\ b_m \end{pmatrix}.$$

Thus

$$\begin{pmatrix} a_{m+1} \\ b_{m+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -k_m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -k_{m-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -k_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

We apply Euclid's algorithm: We have

$$a_1 = 803 = 5 \cdot 154 + 33 = 5b_1 + 33$$

$$a_2 = 154 = 4 \cdot 33 + 22 = 4b_2 + 22$$

$$a_3 = 33 = 1 \cdot 22 + 11 = 1 \cdot b_3 + 11$$

$$a_4 = 22 = 2 \cdot 11 + 0 = 2b_4 + 0$$

$$a_5 = 11, b_5 = 0$$

Thus $\gcd(803, 154) = a_5 = 11$.

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 $\lambda = 6$, $\mu = -26$ 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 $\lambda = 6$, $\mu = -26$ work.

QUIZ 2. a) State Euclid's Lemma.

b) Define Mersenne primes.

c) Let p be a prime and n an integer such that $p^3|n^4$. Prove that $p^2|n$.

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) Mersenne primes are prime numbers of the form $2^p - 1$ for some prime p.

c) We will use the function e_p. Since $p^4|n^3$, we have $e_p(p^4) \leq e_p(n^3)$. Note that $e_p(p^4) = 4$ and $e_p(n^3) = 3e_p(n)$. Thus $4 \leq 3e_p(n)$. It follows that $e_p(n) > 1$ and since it is an integer, we have $e_p(n) \geq 2$. This means that $p^2|n$.

Second method. We have $p|n^4$. By Euclid's Lemma, $p|n$. Write $n = pm$. Then $(pm)^3 = p^4k$ for some integer k. Thus $m^3 = pk$. It follows that $p|m^3$ and therefore $p|m$, again by Euclid's Lemma. Thus $m = pm_1$ for some integer m_1 and $n = pm = p^2m_1$. Hence $p^2|n$.

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

b) Find the inverse of 23 modulo 67.

c) Find all solutions to the congruence $9x \equiv 6(\mod 15)$.

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 an inverse of 23 modulo 67.

c) Clearly $\gcd(9, 15) = 3$. Since $3|6$, the congrunce will have 3 solutions modulo 15. We first solve the congruence $3x \equiv 2 (\mod 5)$. As 2 is the inverse of 3 modulo 5, we have $x \equiv 2 \cdot 3x \equiv 4 (\mod 5)$. Thus the solutions to our original congruence are 4, $4 + 5 = 9$, and $9 + 5 = 14$.

QUIZ 4. a) Define the Euler function.

b) State Fermat's Little Theorem.

c) Prove that $n^7 \equiv n (\mod 21)$ for every integer n.

Solution: a) The **Euler 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 i

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

b) **Fermat's Little Theorem:** Let p be a prime number. If a is an integer and $p \nmid a$ then $a^{p-1} \equiv 1 (\mod p)$.

An equivalent, but often useful, way of stating FLT is

Fermat's Little Theorem: Let p be a prime number. Then $a^p \equiv a (\mod p)$ for any integer a.

c) We use the following simple, but useful, observation. If $\gcd(m, n) = 1$ then the congruence $a \equiv b (\mod mn)$ is equivalent to the pair of congruences
$a \equiv b (\mod m)$ and $a \equiv b (\mod n)$ (in other words, an integer is divisible by mn if and only if it is divisible by both m and n).

Since $21 = 3 \cdot 7$ and $\gcd(3,7) = 1$, it suffices to show that for every integer n we have $n^7 \equiv n (\mod 7)$ and $n^7 \equiv n (\mod 3)$. The first congruence is true by Fermat's Little Theorem for the prime 7.

By FLT for the prime 3 we have $n^3 \equiv n (\mod 3)$. Squaring each side of this congruence and then multiplying both sides by n we get

$$n^7 = n(n^3)^2 \equiv n \cdot n^2 = n^3 \equiv n(\mod 3).$$

This completes our proof.

Remark. Note that $n^7 \equiv n (\mod 2)$ for any n, so we have a stronger congruence $n^7 \equiv n (\mod 42)$.

QUIZ 5. a) Define primitive root modulo m.

b) a is a primitive root modulo 17.

1. What is $\mathrm{ord}_{17} a^{12}$?
2. What is a^8?

Solution. a) An integer a is a primitive root modulo m if $\gcd(a,m) = 1$ and the order of a modulo m is equal to $\phi(m)$. In other words, $\phi(m)$ is the smallest positive integer k such thaat $a^k \equiv 1 (\mod m)$.

b) Recall the following formula:

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

Since 17 is a prime, we have $\phi(17) = 16$ and $\mathrm{ord}_{17}(a) = 16$. Thus

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

This answers part 1. For part 2, note that

$$(a^8)^2 = a^{16} \equiv 1(\mod 17).$$

Thus a^8 is a solution to $x^2 \equiv 1 (\mod 17)$. The last congruence has only two solutions : 1 and -1 (this is true for any prime modulus). Since a is a primitive root modulo 17, a^8 is not 1 modulo 17. Thus $a^8 \equiv -1 (\mod 17)$.

QUIZ 6. a) State Lagrange's theorem (about polynomial congruences).

b) When does a primitive root modulo m exist?

c) Is 7 a third power residue modulo 13?

Solution. a) **Lagrange's Theorem.** Let p be a prime number and $f(x) = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_0$ a polynomial with integer coefficients such that $p \nmid a_k$. Then the congruence $f(x) \equiv 0(\mod p)$ has at most k different solutions modulo p.

b) A primitive root modulo m exists if and only if m is one of the numbers $1, 2, 4, p^k, 2p^k$, where p is an odd prime and k a positive integer.

c) Recall the following theorem: Suppose that there is a primitive root modulo m. An integer a is a k-th power residue modulo m (i.e. the congurnce $x^k \equiv a(\mod m)$ is solvable) if and only if

$$a^{\phi(m)/\gcd(k,\phi(m))} \equiv 1(\mod m)$$

.

Since 13 is a prime, a primitive root modulo 13 exists. We apply the theorem to the case $m = 13$, $k = 3$, $a = 7$. Thus $\phi(m) = 12$ and $\phi(m)/\gcd(k, \phi(m)) = 4$. However

$$7^4 = 49^2 \equiv (-3)^2 = 9 \not\equiv 1(\mod 13)$$

so 7 is not a third power residue modulo 13.

QUIZ 7. a) Define the Legendre's symbol.

b) State the quadratic reciprocity.

c) 2017 is a prime number. Using Jacobi symbol computations determine whether 1006 is a square modulo 2017.

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

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

b) 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.

c) We have $1006 = 2 \cdot 503$. Also, $2017 \equiv 1 \pmod 8$. Thus

$$\left(\frac{1006}{2017}\right) = \left(\frac{2}{2017}\right)\left(\frac{503}{2017}\right) = \left(\frac{503}{2017}\right).$$

Using Jacobi symbol reciprocity and the fact that $2017 \equiv 5 \pmod{503}$, we have

$$\left(\frac{503}{2017}\right) = \left(\frac{2017}{503}\right) = \left(\frac{5}{503}\right) = \left(\frac{503}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

(we used the observation that in each symbol at lest one number was congruent to 1 mod 4).

We computed that $\left(\frac{1006}{2017}\right) = -1$, hence 1006 is a quadratic non-residue modulo 2017, i.e. it is not a suqare modulo 2017.

QUIZ 8. a) Define the convolution $f * g$ of two arithmetic functions and list its main properties.

b) Let $f(n) = \lfloor n/2 \rfloor$. Compute $(f*\mathbb{1})(20)$, where $\mathbb{1}$ is the constant function $\mathbb{1}(n) = 1$ for all n.

c) Let $f(n) = n$. Find a closed formula for $f * f$ in terms of a function we discussed in class.

Solution. a) 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. the convolution of two multiplicative functions is multiplicative

6. 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.

7. the convolution inverse of a multiplicative function f is multiplicative, i.e. if $f * g = \delta$ then g is multiplicative.

8. 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 $g = 0$.

9. 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

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

10. 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) The positive divisors of 20 are $1, 2, 4, 5, 10, 20$. Thus

$$(f * \mathbb{1})(20) = f(1)\mathbb{1}(20) + f(2)\mathbb{1}(10) + f(4)\mathbb{1}(5) + f(5)\mathbb{1}(4) + f(10)\mathbb{1}(2) + f(20)\mathbb{1}(1) =$$

$$= \lfloor 1/2 \rfloor + \lfloor 2/2 \rfloor + \lfloor 4/2 \rfloor + \lfloor 5/2 \rfloor + \lfloor 10/2 \rfloor + \lfloor 20/2 \rfloor = 20.$$

c) We have

$$f * f(n) = \sum_{d|n} f(d) f(n/d) = \sum_{d|n} d\frac{n}{d} = \sum_{d|n} n = n \sum_{d|n} 1 = n\nu(n).$$

Thus $f * f(n) = n\nu(n)$ for all n. Recall that $\nu = \mathbb{1} * \mathbb{1}$ and $\nu(n)$ is the number of positive divisors of n.

QUIZ 9. a) Define a finite simple continued fraction.

b) Express $\frac{43}{40}$ as a finite simple continued fraction.

c) Which is bigger:

1. $[2, 1, 3, 4, 7, 2]$ or $[2, 1, 3, 5, 7, 1]$?

2. $[2, 1, 1, 1, 1]$ or $[2, 1, 1, 2]$?

Solution. a) A finite simple continued fraction is an expression of the form

$$[k_0, k_1, \ldots, k_s] = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\cdots + \cfrac{1}{k_s}}}}$$

where k_0 is an integer and $k_1, \ldots, k_s$ are positive integers.

b) 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

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

c) Recall the following result. Suppose that $[k_0, k_1, \ldots, k_s]$ and $[l_o, l_1, \ldots, l_t]$ are two finite simple continued fractions which **are not equal**. Suppose there are 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

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

The two continued fractions in 1. are not euqal and the first place they differ is $r = 3$. Since 3 is odd, the continued fraction with bigger k_3 is smaller, i.e.

$$[2, 1, 3, 4, 7, 2] > [2, 1, 3, 5, 7, 1].$$

The two continued fractions in 2. are equal, as we know that

$$[k_0, k_1, \ldots, k_s] = [k_0, k_1, \ldots, k_s - 1, 1]$$

(and this is the only way two finite simple continued fractions can be equal).

QUIZ 10. a) Define an infinite simple continued fraction and its convergents.

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

c) Express $\sqrt{5}$ as simple countinued fraction.

Solutions. 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) 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) Rexall that if $x_0 = \sqrt{5}$, $x_{n+1} = \dfrac{1}{x_n - \lfloor x_n \rfloor}$ and $k_n = \lfloor x_n \rfloor$ then $x_0 = [k_0, k_1, \ldots]$. We have $k_0 = \lfloor x_0 \rfloor = 2$,

$$x_1 = \frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2, \quad k_1 = \lfloor x_1 \rfloor = 4, \quad x_2 = \frac{1}{(\sqrt{5} + 2) - 4} = x_1.$$

We see that $x_1 = x_2$, which means that $x_1 = x_2 = x_3 = \ldots$ and $k_1 = k_2 = \ldots = 4$. Thus

$$\sqrt{5} = [2, 4, 4, 4, \ldots].$$

QUIZ 11. a) How many solutions in positive integers does the the equation $5x + 7y = 88$ have?

b) Which integers are sums of two squares?

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

d) Find a right-angled triangle with integral side-lengths and hypotenuse of length 29.

Solution. a) Note that $\gcd(5, 7) = 1$. We first find u, w such that $5u + 3w = 1$. This is usually done via Euclidean algorithm, but in our case we can easily guess that $u = 3, w = -2$ works. Multiplying by 88, we see thta $x_0 = 3 \cdot 88 = 264$, $y_0 = (-2) \cdot 88 = -176$ is a solution to our equation. It follows that all solutions are described by $x = 264 + 7k$, $y = -176 - 5k$, $k \in \mathbb{Z}$. We want both x and y to be positive. Now, $264 + 7k > 0$ iff $k > -264/7 = -37\frac{5}{7}$. Similarly, $-176 - 5k > 0$ iff $k < -176/5 = -35\frac{1}{5}$. The only integers k which satisfy

$$-37\frac{5}{7} < k < -35\frac{1}{5}$$

are $k = -37$ and $k = -36$. Thus we have exactly two solutions in positive integers:

$$x = 264 + 7(-37) = 5, y = -176 - 5(-37) = 9$$

and

$$x = 264 + 7(-36) = 12, y = -176 - 5(-36) = 4.$$

b) A positive integer n is a sum of two squares if and only if every prime divisor of n of the form $4k + 3$ appears in the prime factorization of n to an even power.

c) Recall the identity $(a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2$. Note that $13 = 3^2+2^2$ and $17 = 4^2 + 1^2$. Thus

$$13 \cdot 17 = (3 \cdot 4 + 2 \cdot 1)^2 + (3 \cdot 1 - 2 \cdot 4)^2 = 14^2 + 5^2.$$

We have another solution

$$13 \cdot 17 = (3 \cdot 1 + 2 \cdot 4)^2 + (3 \cdot 4 - 2 \cdot 1)^2 = 11^2 + 10^2.$$

d) The problem asks to find a Pythagorean triple of the form $(a, b, 29)$. Since 29 is a prime, any such triple must be primitive. We may assume b is even. Thus there are positive, relatively prime integers $m < n$ of different parities such that $29 = m^2 + n^2$, $b = 2mn$, $a = n^2 - m^2$. We easily find $n = 5$, $m = 2$ is the only solution, hence $a = 21$, $b = 20$.