WORKSHEET #1

Definition 1. *A triple* (a, b, c) *of natural numbers is a* ***Pythagoran triple*** *if they form the side lengths of a right triangle, where* c *is the length of the hypotenuse.*

Theorem 2 (Fundamental Theorem of Arithmetic)**.** *Every natural number* $n \geq 1$ *can be written as a product of prime numbers:*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

This expression is unique up to reordering. □

Definition 3. *We call the number* e_i *the* ***multiplicity*** *of the prime* p_i *in the prime factorization of*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Definition 4. *Let* m, n *be integers and* $K \geq 1$ *be a natural number. We say that* m ***is congruent to*** n ***modulo*** K*, written as* $m \equiv n \pmod{K}$*, if* $m - n$ *is a multiple of* K*.*

Theorem 5. *Let* n *be an integer and* $K \geq 1$ *a natural number. Then* n *is congruent to exactly one nonnegative integer between* 0 *and* $K - 1$*: this number is the "remainder" when you divide* n *by* K*.* □

Proposition 6. *Let* m, m', n, n' *and* K *be natural numbers. Suppose that*

$$m \equiv m' \pmod{K} \quad \text{and} \quad n \equiv n' \pmod{K}.$$

Then

$$m + n \equiv m' + n' \pmod{K} \quad \text{and} \quad mn \equiv m'n' \pmod{K}.$$ □

Definition 7. *A triple* (a, b, c) *of natural numbers is a* ***primitive Pythagoran triple (PPT)*** *if* $a^2 + b^2 = c^2$*, and there is no common factor of* a, b, c *greater than* 1*; equivalently,* a, b, c *have no common prime factor.*

Theorem 8. *The set of primitive Pythagorean triples* (a, b, c) *with* a *odd is given by the formula*

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

where $s > t \geq 1$ *are odd integers with no common factors.*

Theorem 9. *The set of points on the unit circle* $x^2 + y^2 = 1$ *with positive rational coordinates is given by the formula*

$$(x, y) = \left(\frac{2v}{v^2 + 1}, \frac{v^2 - 1}{v^2 + 1} \right)$$

where v *ranges through rational numbers greater than one.*

WORKSHEET #2

Definition 10. *The* ***greatest common divisor*** *of two integers* a *and* b*, denoted* $\gcd(a, b)$*, is the largest integer that divides* a *and* b*.*

Definition 11. *Two integers* a *and* b *are* ***coprime*** *if* $\gcd(a, b) = 1$*.*

Theorem 12. *The Euclidean algorithm terminates and outputs the correct value of* $\gcd(a, b)$*.*

Definition 13. *An expression of the form* $ra + sb$ *with* $r, s \in \mathbb{Z}$ *is a* ***linear combination*** *of* a *and* b*.*

Corollary 14. *If* a, b *are integers, then* $\gcd(a, b)$ *can be realized as a linear combination of* a *and* b*. Concretely, we can use the Euclidean algorithm to do this.*

Theorem 15. *Let a, b, c be integers. The equation*

$$ax + by = c$$

has an integer solution if and only if c is divisible by $d := \gcd(a, b)$. If this is the case, there are infinitely many solutions. If (x_0, y_0) is a one particular solution, then the general solution is of the form

$$x = x_0 - (b/d)n, \quad y = y_0 + (a/d)n$$

as n ranges through all integers.

PROBLEM SET #1

Lemma 16. *Lat a, b, c be integers. If a and b are coprime, and a divides bc, then a divides c.*

WORKSHEET #3

Definition 17. *A **congruence class** modulo K is a set of the form*

$$[a] := \{n \in \mathbb{Z} \mid n \equiv a \pmod{K}\}$$

for some $a \in \mathbb{Z}$.

Definition 18. *A **representative** for a congruence class is an element of the congruence class.*

Proposition 19. *Given $K > 0$, the set of integers $\mathbb{Z}$ is the disjoint union of K congruence classes:*

$$\mathbb{Z} = [0] \sqcup [1] \sqcup \cdots \sqcup [K-1].$$

Definition 20. *The ring $\mathbb{Z}_K$ is the set of congruence classes modulo K:*

$$\{[0], [1], \dots, [K-1]\}$$

equipped with the operations

$$[a] + [b] = [a + b] \quad \textit{and} \quad [a][b] = [ab].$$

Definition 21. *We say that a number a is a **unit modulo** K if there is an integer solution x to $ax \equiv 1 \pmod{K}$, and we say that such a number x is an **inverse modulo** K to a.*

Definition 22. *We say that a congruence class $[a]$ is a **unit in** $\mathbb{Z}_K$ if there is a congruence class $x \in \mathbb{Z}_K$ such that $[a]x = [1]$, and we say that such a class x is an **inverse** to $[a]$ in $\mathbb{Z}_K$.*

Theorem 23. *Let a and n be integers, with n positive. Then a is a unit modulo n if and only if a and n are coprime.*

Theorem 24 (Chinese Remainder Theorem)**.** *Given $m_1, \dots, m_k > 0$ integers such that m_i and m_j are coprime for each $i \neq j$, and $a_1, \dots, a_k \in \mathbb{Z}$, the system of congruences*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \qquad\qquad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

has a solution $x \in \mathbb{Z}$. Moreover, the set of solutions forms a unique congruence class modulo $m_1 m_2 \cdots m_k$.

PROBLEM SET #2

Lemma 25. *Lat a, b, c be integers. If a and b are coprime, a divides c, and b divides c, then a divides bc.*

Definition 26. *Given integers $a_1, \dots, a_m$, the **greatest common divisor** of $a_1, \dots, a_m$ is the largest integer that divides all of them.*

Theorem 27. *Let a, b, n be integers, with $n > 0$. Then $[a]x = [b]$ has a solution x in $\mathbb{Z}_n$ if and only if $\gcd(a, n)$ divides b. In this case, the number of distinct solutions is exactly $\gcd(a, n)$.*

Worksheet #4

Definition 28. *A **group** is a set G equipped with a product operation*

$$G \times G \to G \qquad (g,h) \mapsto gh$$

*and an **identity** element $1 \in G$ such that*

- *the product is associative: $(gh)k = g(hk)$ for all $g,h,k \in G$,*
- *$g1 = 1g = g$ for all $g \in G$, and*
- *for every $g \in G$, there is an inverse element $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1$.*

Definition 29. *A group is **abelian** if the product is commutative: $gh = hg$ for all $g,h \in G$.*

Definition 30. *A **finite group** is a group G that is a finite set.*

Definition 31. *Let G be a group and $g \in G$. The **order** of g is the smallest positive integer n such that $g^n = e$, if some such n exists, and ∞ if no such integer exists.*

Theorem 32 (Lagrange's Theorem)**.** *Let G be a finite group and $g \in G$. Then the order of g is finite and divides the cardinality of the group G.*

Theorem 33 (Fermat's Little Theorem)**.** *Let p be a prime number and a an integer. If p does not divide a, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Definition 34. *Let n be a positive integer. We define $\varphi(n)$ to be the number of elements of $\mathbb{Z}_n^\times$. We call this **Euler's phi function**.*

Proposition 35. *Euler's phi function satisfies the following properties.*

(1) If p is a prime and n is a positive integer, then $\varphi(p^n) = p^{n-1}(p-1)$.
(2) If m,n are coprime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Theorem 36 (Euler's Theorem)**.** *Let a,n be coprime integers, with n positive. Then*

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

Worksheet #5

Proposition 37. *Let p be a prime. Let $p(x)$ be a polynomial of degree d with coefficients in $\mathbb{Z}_p$. Then $p(x)$ has at most d roots in $\mathbb{Z}_p$.* □

Lemma 38. *If G is a group, $g \in G$, and n a positive integer such that $g^n = 1$, then the order of g divides n.*

Definition 39. *Let n be a positive integer. An element $x \in \mathbb{Z}_n^\times$ is a **primitive root** if the order of x in $\mathbb{Z}_n^\times$ equals $\phi(n)$ (the cardinality of $\mathbb{Z}_n^\times$).*

Theorem 40. *Let p be a prime number. Then there exists a primitive root in $\mathbb{Z}_p^\times$.*

Definition 41. *If $[a]$ is a primitive root in $\mathbb{Z}_p$, the function*

$$\mathbb{Z}_p^\times \to \mathbb{Z}_{p-1} \qquad [b] \mapsto [m] \text{ such that } [b] = [a]^m$$

*is called the **discrete logarithm** or **index** of $\mathbb{Z}_p^\times$ with base $[a]$.*

Lemma 42. *Let p be a prime and $[a]$ a primitive root in $\mathbb{Z}_p$. The corresponding discrete logarithm function $I : \mathbb{Z}_p^\times \to \mathbb{Z}_{p-1}$ satisfies the property*

$$I(xy) = I(x) + I(y) \quad \text{and} \quad I(x^n) = [n]I(x)$$

for $x,y \in \mathbb{Z}_p^\times$ and $n \in \mathbb{N}$.

Proposition 43. *Let n be a positive integer. Then* $\sum_{d \mid n} \varphi(d) = n$.

Theorem 44. *Let p be a prime. Suppose that there are n distinct solutions to $x^n = 1$ in $\mathbb{Z}_p$. Then $\mathbb{Z}_p^\times$ has exactly $\varphi(n)$ elements of order n.*

WORKSHEET #6

Definition 45. *We say that an element $x \in \mathbb{Z}_n$ is a **square** or a **quadratic residue** if there is some $y \in \mathbb{Z}_n$ such that $y^2 = x$, and in this case, we call y a **square root** of x.*

Definition 46. *Let p be an odd prime. For $r \in \mathbb{Z}$ not a multiple of p we define the **Legendre symbol** of r with respect to p as*

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \text{if } [r] \text{ is a square in } \mathbb{Z}_p, \\ -1 & \text{if } [r] \text{ is a not square in } \mathbb{Z}_p. \end{cases}$$

Theorem 47 (Euler's Criterion)**.** *For p an odd prime and $r \in \mathbb{Z}$ not a multiple of p, we have*

$$\left(\frac{r}{p}\right) \equiv r^{(p-1)/2} \pmod{p}.$$

Theorem 48 (Quadratic Reciprocity part -1)**.** *If p is odd, then*

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

Proposition 49. *Let p be an odd prime and a, b integers not divisible by p. Then*

(1) $a \equiv b \pmod{p}$ *implies that* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
(3) $\left(\frac{a^2}{p}\right) = 1$.

PROBLEM SET #3

Theorem 50. *If p is an odd prime and $n > 0$, then $\mathbb{Z}_{p^n}$ has a primitive root.*

WORKSHEET #7

Theorem 51 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \qquad \text{if either } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4},$$
$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \qquad \text{if both } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}.$$

Theorem 52 (Quadratic Reciprocity part 2)**.** *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = 1 \qquad \text{if } p \equiv \pm 1 \pmod{8},$$
$$\left(\frac{2}{p}\right) = -1 \qquad \text{if } p \equiv \pm 3 \pmod{8}.$$

Lemma 53 (Gauss' Lemma)**.** *Let p be an odd prime and set $p' = \frac{p-1}{2}$. Note that every integer coprime to p is congruent modulo p to a unique integer in the set $S = \{\pm 1, \pm 2, \cdots, \pm p'\}$.*

Let a be an integer coprime to p. Consider the sequence

$$a, 2a, 3a, \ldots, p'a$$

and replace each element in the sequence with element of S that is congruent with modulo p to get a list L of p'-many elements of S.

Then $\left(\dfrac{a}{p}\right) = (-1)^\nu$, where ν is the number of negative integers in L.

Lemma 54. *Let p and q be two coprime odd positive integers. Then*

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

WORKSHEET #8

Theorem 55 (Euclid)**.** *There are infinitely many primes.*

Proposition 56. *For each of the following conditions, there are infinitely many primes p:*

- $p \equiv 1 \pmod 3$
- $p \equiv 2 \pmod 3$
- $p \equiv 1 \pmod 4$
- $p \equiv 3 \pmod 4$

WORKSHEET #9

Theorem 57. *An odd prime is a sum of two squares if and only if it is congruent to 1 modulo 4.*

Theorem 58 (Sums of Two Squares Theorem)**.** *A positive integer n is a sum of two squares if and only if: for every prime p such that $p \equiv 3 \pmod 4$ and p divides n, the multiplicity of p in the prime factorization of n is even.*

WORKSHEET #10

Definition 59. *A **finite continued fraction** is an expression of the form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

for some integers $a_0 \in \mathbb{Z}, a_1, \ldots, a_n \in \mathbb{Z}_{>0}$. We write $[a_0; a_1, \ldots, a_n]$ as shorthand for this.

*An **infinite continued fraction** is an expression of the form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

for some integers $a_0 \in \mathbb{Z}, a_1, a_2, a_3, \ldots \in \mathbb{Z}_{>0}$.
We write $[a_0; a_1, a_2, \ldots]$ as shorthand for this.

*By a **continued fraction** we mean either an infinite or finite continued fraction. We call the numbers a_i the **partial quotients** in the continued fraction.*

Definition 60. *Given an infinite continued fraction $[a_0; a_1, a_2, \ldots]$, the k-th **convergent** of the continued fraction is the value C_k of the finite continued fraction $[a_0; a_1, \ldots, a_k]$.*

Theorem 61. *Every infinite continued fraction converges to a real number; i.e., for any* $[a_0; a_1, a_2, a_3, \ldots]$ *with* $a_0 \in \mathbb{Z}$ *and* $a_1, a_2, \ldots \in \mathbb{Z}_{>0}$*, the sequence of convergents* $C_1, C_2, C_3, \ldots$ *converges. We call this limit the value of the infinite continued fraction.*

Algorithm 62 (Continued Fraction Algorithm)**.** *Given a real number* r*,*

(I) Start with $\beta_0 := r$ *and* $n := 0$*.*

(II) Set $a_n := \lfloor \beta_n \rfloor$*.*

(III) If $a_n = \beta_n$*, STOP; the continued fraction is* $[a_0; a_1, \ldots, a_n]$*.*
Else, set $\beta_{n+1} := (\beta_n - a_n)^{-1}$*, and return to Step (**??**).*

If the algorithm does not terminate, the continued fraction is $[a_0; a_1, a_2, \ldots]$*.*

Theorem 63. *For any real number* r*, the continued fraction obtained from the Continued Fraction Algorithm with input* r *converges to* r*.*

Proposition 64. *Let* r *be a real number. The Continued Fraction Algorithm with input* r *terminates in finitely many steps if and only if* r *is rational.*

Theorem 65 (Dirichlet Approximation Theorem)**.** *Let* $r = [a_0; a_1, a_2, a_3, \ldots]$ *be a real number. Then for every convergent* $C_k = \dfrac{p_k}{q_k}$ *(in lowest terms), we have* $\left| r - \dfrac{p_k}{q_k} \right| < \dfrac{1}{q_k^2}$*.*

In particular, if r *is irrational, there are infinitely many rational numbers* $\dfrac{p}{q}$ *such that* $\left| r - \dfrac{p}{q} \right| < \dfrac{1}{q^2}$*.*

Proposition 66. *Let* $[a_0; a_1, a_2, \ldots]$ *be a continued fraction. Set*

$$\begin{aligned} p_0 &:= a_0, & p_1 &:= a_0 a_1 + 1, & p_k &:= a_k p_{k-1} + p_{k-2} \\ q_0 &:= 1, & q_1 &:= a_1, & q_k &:= a_k q_{k-1} + q_{k-2}. \end{aligned}$$

Then,

(1) $C_k = \dfrac{p_k}{q_k}$ *for all* $k \geq 0$*, and*

(2) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ *for all* $k \geq 1$*.*

PROBLEM SET #5

Theorem 67. *Let* r *be a real number,* $C_k = \frac{p_k}{q_k}$ *be the* k*-th convergent of* r*, and* $\frac{p}{q} \neq r$ *be a rational number, with* $q > 0$*. If* $q < q_k$*, then* $\left| r - \dfrac{p}{q} \right| > \left| r - \dfrac{p_k}{q_k} \right|$*.*

WORKSHEET #11

Definition 68. *The equation* $x^2 - Dy^2 = 1$ *for some fixed positive integer* D *that is not a perfect square, where the variables* x, y *range through integers is called a* ***Pell's equation****. We say that a solution* (x_0, y_0) *is a* ***positive solution*** *if* x_0, y_0 *are both positive integers. We say that one positive solution* (x_0, y_0) *is* ***smaller*** *than another positive solution* (x_1, y_1) *if* $x_0 < x_1$*; equivalently,* $y_0 < y_1$*.*

Definition 69. *Let* D *be a positive integer that is not a perfect square. We define the* ***quadratic ring*** *of* D *to be*

$$\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}.$$

Definition 70. *For the quadratic ring* $\mathbb{Z}[\sqrt{D}]$ *we define the* ***norm*** *function*

$$N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z} \qquad N(a + b\sqrt{D}) = a^2 - b^2 D.$$

Note that $N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D})$*.*

Lemma 71. *For the quadratic ring $\mathbb{Z}[\sqrt{D}]$ the norm function satisfies the multiplicative property $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Theorem 72. *Let D be a positive integer that is not a perfect square. Consider the Pell's equation $x^2 - Dy^2 = 1$. Let (a, b) be the smallest positive solution (assuming that some positive solution exists). Then every positive solution (c, d) can be obtained by the rule*

$$c + d\sqrt{D} = (a + b\sqrt{D})^k$$

for some positive integer k.

WORKSHEET #12

Theorem 73. *Let D be a positive integer that is not a perfect square. Then the Pell's equation $x^2 - Dy^2 = 1$ has a positive solution.*

Theorem 74. *Let D be a positive integer that is not a perfect square. For every positive solution (a, b) to the Pell's equation $x^2 - Dy^2 = 1$, there is some $k \in \mathbb{Z}_{\geq 0}$ such that the ratio $\frac{a}{b}$ is a convergent C_k of the continued fraction of $\sqrt{D}$.*

Theorem 75. *Let r be an irrational real number. If p, q are integers with $q > 0$ such that $|r - \frac{p}{q}| < \frac{1}{2q^2}$, then there is some $k \in \mathbb{Z}_{\geq 0}$ such that $\frac{p}{q}$ is a convergent C_k of the continued fraction of r.*

PROBLEM SET #5

Theorem 76. *Let r be a real number, $C_k = \frac{p_k}{q_k}$ be the k-th convergent of r, and $\frac{p}{q} \neq r$ be a rational number, with $q > 0$. If $q < q_k$, then $\left|r - \dfrac{p}{q}\right| > \left|r - \dfrac{p_k}{q_k}\right|$.*

WORKSHEET #13

Definition 77. *A **triangular number** is a natural number T_n that counts the number of dots in a triangular array with n elements along the base.*

Definition 78. *A **pentagonal number** is a natural number P_n that counts the number of dots in a pentagonal array (with a fixed corner) with n elements along the base.*

Definition 79. *A **centered hexagonal number** is a natural number H_n that counts the number of dots in a hexagonal array (with a fixed center) with n elements along the base.*

WORKSHEET #14

Definition 80. *A (real) **elliptic curve** is the solution set E in $\mathbb{R}^2$ to an equation of the form $y^2 = x^3 + ax + b$ for real constants $a, b \in \mathbb{R}$ that satisfy the technical assumption that $4a^3 + 27b^2 \neq 0$. For an elliptic curve E we define $\overline{E} = E \cup \{\infty\}$, where ∞ is a formal symbol.*

Definition 81. *For an elliptic curve E, and points $P, Q \in E$ with $P \neq Q$, we set:*

$$\begin{aligned}
P^\vee &:= \text{the reflection of } P \text{ over the } x\text{-axis} \\
P \star Q &:= R^\vee, \text{ where } R \text{ is the third point of intersection of the line between } P \text{ and } Q \text{ and } E \\
P \star P &:= S^\vee, \text{ where } S \text{ is the other point of intersection of the tangent line to } E \text{ at } P \text{ and } E.
\end{aligned}$$

Theorem 82. *There is a group structure on $\overline{E}$ with operation $\star$, identity element ∞, and inverse $-^\vee$.*

WORKSHEET #15

Theorem 83. *If E is a real elliptic curve given by the equation $y^2 = x^3 + ax + b$ for rational numbers $a, b \in \mathbb{Q}$, then the set of rational points on E (along with the infinity point "∞") form a group with operation $\star$, identity element ∞, and inverse $-^{\vee}$. We denote this group by $E_{\mathbb{Q}}$.*

WORKSHEET #16

Definition 84. *Let $p \geq 5$ be a prime. An* ***elliptic curve*** *over $\mathbb{Z}_p$ is the solution set E_p in $\mathbb{Z}_p \times \mathbb{Z}_p$ to an equation of the form $y^2 = x^3 + [a]x + [b]$ for real constants $[a], [b] \in \mathbb{Z}_p$ that satisfy the technical assumption that $[4][a]^3 + [27][b]^2 \neq 0$. For an elliptic curve E_p we define $\overline{E}_p = E_p \cup \{\infty\}$, where ∞ is a formal symbol.*

Theorem 85. *There is a group structure on $\overline{E}_p$ with operation $\star$, identity element ∞, and inverse $-^{\vee}$ given by the same geometric rules as in the real case.*