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*

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

Then

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

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:*

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

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 $m_1, \ldots, m_k > 0$ integers such that m_i and m_j are coprime for each $i \neq j$, and $a_1, \ldots, a_k \in \mathbb{Z}$, 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 $m_1 m_2 \cdots m_k$.