Elementary Number Theory
Math 175, Section 30, Autumn 2010
Shmuel Weinberger (shmuel@math.uchicago.edu)
Tom Church (tchurch@math.uchicago.edu)
www.math.uchicago.edu/~tchurch/teaching/175/

Script 1: Divisibility in the Integers

Definition 1.1. Let $\mathbb{Z}$ be the *integers*, that is, the unique ordered commutative ring with identity whose positive elements satisfy the well-ordering property. In other words, the integers satisfy the following axioms:

E1. (Reflexivity, Symmetry, and Transitivity of Equality)

Reflexivity of Equality	If $a \in \mathbb{Z}$, then $a = a$.
Symmetry of Equality	If $a, b \in \mathbb{Z}$ and $a = b$, then $b = a$.
Transitivity of Equality	If $a, b, c \in \mathbb{Z}$ and $a = b$ and $b = c$, then $a = c$.

E2. (Additive Property of Equality)

If $a, b, c \in \mathbb{Z}$ and $a = b$, then $a + c = b + c$.

E3. (Multiplicative Property of Equality)

If $a, b, c \in \mathbb{Z}$ and $a = b$, then $a \cdot c = b \cdot c$.

A1. (Closure of Addition)

If $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$.

A2. (Associativity of Addition)

If $a, b, c \in \mathbb{Z}$, then $(a + b) + c = a + (b + c)$.

A3. (Commutativity of Addition)

If $a, b \in \mathbb{Z}$, then $a + b = b + a$.

A4. (Additive Identity)

There is an element $0 \in \mathbb{Z}$ such that $a + 0 = a$ and $0 + a = a$ for every $a \in \mathbb{Z}$.

A5. (Additive Inverses)

For each element $a \in \mathbb{Z}$, there is a unique element $-a \in \mathbb{Z}$ such that $a + (-a) = 0$ and $(-a) + a = 0$.

M1. (Closure of Multiplication)

If $a, b \in \mathbb{Z}$, then $a \cdot b \in \mathbb{Z}$.

M2. (Associativity of Multiplication)

If $a, b, c \in \mathbb{Z}$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

M3. (Commutativity of Multiplication)

If $a, b \in \mathbb{Z}$, then $a \cdot b = b \cdot a$.

M4. (Multiplicative Identity)

There is an element $1 \in \mathbb{Z}$ (with $1 \neq 0$) such that $a \cdot 1 = a$ and $1 \cdot a = a$ for every $a \in \mathbb{Z}$.

D. (Distributivity of Multiplication over Addition)

If $a, b, c \in \mathbb{Z}$, then $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

O1. (Transitivity of Inequality)

If $a, b, c \in \mathbb{Z}$ and $a < b$ and $b < c$, then $a < c$.

O2. (Trichotomy)

If $a, b \in \mathbb{Z}$, then exactly one of the following is true: $a < b$, $a = b$, or $a > b$.

O3. (Additive Property of Inequality)

If $a, b, c \in \mathbb{Z}$ and $a < b$, then $a + c < b + c$.

O4. (Multiplicative Property of Inequality)

If $a, b, c \in \mathbb{Z}$ and $a < b$ and $c > 0$, then $a \cdot c < b \cdot c$.

W. (Well-Ordering Property)

If S is a non-empty set of positive integers, then S has a least element (that is, there is some $x \in S$ such that if $y \in S$, then $x \leq y$).

To prepare for class on Thursday, September 30: Theorem 1.2 through 1.15.

For Theorems 1.2 through 1.6, you may use Axioms E1–E3, A1–A5, M1–M4, and D.

Theorem 1.2 (Cancellation Law for Addition)**.** If $a + c = b + c$, then $a = b$.

Theorem 1.3. If $a \in \mathbb{Z}$, then $-(-a) = a$.

Theorem 1.4. If $a \in \mathbb{Z}$, then $(-1) \cdot a = -a$.

Theorem 1.5. If $a \in \mathbb{Z}$, then $a \cdot 0 = 0$.

Theorem 1.6. If $a, b \in \mathbb{Z}$, then:

(i) $a(-b) = -ab$ and $(-a)b = -ab$

(ii) $(-a)(-b) = ab$

Challenge Problem 1.7. Prove Theorem 1.2 without assuming that additive inverses are unique (i.e. delete the word "unique" from Axiom A5). Then use Theorem 1.2 to prove that $-a$ is in fact unique anyway.

For Theorems 1.8 through 1.12, you may also use Axioms O1–O4.

Theorem 1.8. If $a > 0$, then $-a < 0$. (And if $a < 0$, then $-a > 0$.)

Theorem 1.9. If $a < b$ and $c < 0$, then $ac > bc$.

Theorem 1.10. If $a \neq 0$, then $a^2 > 0$.

Exercise 1.11. Prove that $1 > 0$.

Theorem 1.12. If $a \geq 1$ and $b > 0$, then $ab \geq b$.

For Theorem 1.13, you may also use Axiom W.

Theorem 1.13. There is no integer between 0 and 1.

Challenge Problem 1.14. Prove that Axiom W is necessary to prove Theorem 1.13.

Theorem 1.15 (Cancellation for Multiplication)**.** If $a \neq 0$ and $a \cdot b = a \cdot c$, then $b = c$.

Definition 1.16. Let $a, b \in \mathbb{Z}$. We say that b *divides* a (and that b is a *divisor* of a) and write $b|a$ provided that there is some $n \in \mathbb{Z}$ such that $a = b \cdot n$.

Definition 1.17 (Division)**.** If $b|a$ (with $b \neq 0$) and c is the integer such that $a = b \cdot c$, then we define $\frac{a}{b} = c$.

Exercise 1.18. Show that $\frac{a}{b}$ is well-defined.

Theorem 1.19. If $a|b$ and $a|c$, then $a|(b+c)$ and $a|(b-c)$.

Theorem 1.20. If $a|b$ and $c \in \mathbb{Z}$, then $a|(b \cdot c)$.

Theorem 1.21. If $a|b$ and $b|c$, then $a|c$.

Exercise 1.22. Prove that if $a|b$ and $a|c$ and $s, t \in \mathbb{Z}$, then $a|(sb + tc)$.

Theorem 1.23. If $a > 0$, $b > 0$ and $a|b$, then $a \leq b$.

Exercise 1.24. Show that any non-zero integer has a finite number of divisors.

Theorem 1.25. If $a|b$ and $b|a$, then $a = \pm b$.

Theorem 1.26. If $m \neq 0$, then $a|b$ if and only if $ma|mb$.

Theorem 1.27. (The Division Algorithm) If $a, b \in \mathbb{Z}$ and $b > 0$, then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Definition 1.28. Let $a, b \in \mathbb{Z}$, not both zero. A *common divisor* of a and b is defined to be any integer c such that $c|a$ and $c|b$. The *greatest common divisor* of a and b is denoted (a, b) and represents the largest element of the set $\{c \in \mathbb{Z} \mid c|a, c|b\}$.

Exercise 1.29. Show that $(a, b) = (b, a) = (a, -b)$.

Theorem 1.30. If $d|a$ and $d|b$, then $d|(a, b)$. (Hint: Do Theorem 1.31 first.)

Theorem 1.31. If $d = (a, b)$, then there exist integers x, y such that $d = xa + yb$.

Theorem 1.32. If $m \in \mathbb{Z}$ and $m > 0$, then $(ma, mb) = m(a, b)$.

Theorem 1.33. If $d|a$ and $d|b$ and $d > 0$, then $(\frac{a}{d}, \frac{b}{d}) = \frac{(a,b)}{d}$.

Definition 1.34. Two integers a and b are said to be *relatively prime* if $(a, b) = 1$.

Theorem 1.35. If $(a, m) = 1$ and $(b, m) = 1$, then $(ab, m) = 1$.

Theorem 1.36. If $c|ab$ and $(c, b) = 1$, then $c|a$.

Theorem 1.37. (The Euclidean Algorithm)

Let $a, b \in \mathbb{Z}$ be positive integers. If we apply the Division Algorithm sequentially as follows:

$$\begin{aligned} a &= bq_1 + r_1 & & 0 < r_1 < b \\ b &= r_1 q_2 + r_2 & & 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 & & 0 < r_3 < r_2 \\ &\vdots & & \\ r_{k-2} &= r_{k-1} q_k + r_k & & 0 < r_k < r_{k-1} \\ r_{k-1} &= r_k q_{k+1} & & \end{aligned}$$

then $r_k = (a, b)$.

Some definitions that will come in handy:

Definition 1.38 (Subtraction)**.** We define the *difference* $a - b$ to be the sum $a + (-b)$.

Definition 1.39 (Absolute value)**.** If $a \in \mathbb{Z}$, we define the *absolute value* of a by the following notation and with the following meaning:

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$