Sheet 20: Modulo

Theorem 1 *Let $a \equiv b \pmod{n}$ if $n \mid b - a$. Then $\equiv$ is an equivalence relation.*

Proof. Let a, b and c be integers. Note that $n \mid a - a$ because $0 \cdot n = 0 = a - a$ so $a \equiv a \pmod{n}$. Let $a \equiv b \pmod{n}$. Then there exists $k \in \mathbb{Z}$ such that $kn = b - a$ and so $-kn = a - b$. Since $-k \in \mathbb{Z}$ we have $n \mid a - b$ so $b \equiv a \pmod{n}$. Now let $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then there exists $k, l \in \mathbb{Z}$ such that $nk = b - a$ and $nl = c - b$. Then $n(l + k) = b - a + c - b = c - a$ so $n \mid c - a$. Thus $a \equiv c \pmod{n}$. Hence we have shown reflexivity, symmetry and transitivity so $\equiv$ is an equivalence relation. $\square$

Definition 2 *The equivalence classes of integers under this relation are called residue classes modulo n. We denote it by Z_n.*

Theorem 3 *There are exactly n residue classes modulo n.*

We first prove a lemma showing that every $x \in \mathbb{Z}$ can be written as $x = an + b$ where $b \in \{0, 1, \ldots, n\}$.

Proof. Let $x \in \mathbb{N} \cup \{0\}$ and let $S = \{0, 1, \ldots, n\}$. Then let $T = \{b \in \mathbb{N} \cup \{0\} \mid \text{there exists } a \in \mathbb{Z} \text{ such that } x = an + b\}$. Then we see that $T \neq \emptyset$ since $x = n(0) + x$ and $x \in \mathbb{N} \cup \{0\}$ and $0 \in \mathbb{Z}$. Then we see there exists a least element m of T and so $x = an + m$ for some $a \in \mathbb{Z}$. If $m \in S$ then we are done. If $m \notin S$ then $m > n$ and so $m - n > 0$. Therefore we can write $x = n(a + 1) + (m - n)$ and so $(m - n) \in T$. But $m - n < m$ and since m is the least element of T this is a contradiction so $m \in S$. Therefore every $x \in \mathbb{N} \cup \{0\}$ can be written as $an + b$ for some $a \in \mathbb{Z}$ and $b \in S$. We now consider the case where $x \in \mathbb{Z} \backslash (\mathbb{N} \cup \{0\})$. We see that $-x = -an - b = n(-a - 1) + (-b + n)$. But if $b \neq 0$ then $-b + n \in S$ and if $b = 0$ then $x = an$ and so $-x = a(-n)$ and so we see that for $x \in \mathbb{Z}$ we can write $x = an + b$ for $n \in \mathbb{Z}$ and $b \in S$. $\square$

Now we prove the original result.

Proof. Let $x \in \mathbb{Z}$ and let $S = \{0, 1, \ldots, n\}$. Then we see that $x = an + b$ and $x - b = an$ for some $a \in \mathbb{Z}$ and $b \in S$. But then $x \equiv a \pmod{n}$ and so $x \in \overline{b}$. Since there are only n possible values for b, we see that there are at most n equivalence classes. If we choose two elements $p, q \in S$ such that $p \neq q$ then without loss of generality we can assume $p > q$ and so $(p - q) \in S$. But then $p - q \neq an$ for some $a \in \mathbb{Z}$ and so p is not equivalent to q modulo n and $\overline{p} \neq \overline{q}$. So no two equivalence classes are the same. Additionally, for every $p \in S$ we see that $p = n(0) + p$ and since $0 \in \mathbb{Z}$ and $p \in S$, we see every element of p is in an equivalence class. So we see that there are at least n and at most n equivalence classes so there must be exactly n equivalence classes. $\square$

Definition 4 *For $a, b \in Z_n$ let $x \in a$, $y \in b$ and let*

$$a + b = \overline{(x + y)}$$

$$a \cdot b = \overline{(x \cdot y)}$$

where $\overline{z}$ denotes the residue class of $z \in \mathbb{Z}$.

Theorem 5 *The operations $+$ and $\cdot$ are well-defined on Z_n. Also $(Z_n, +, \cdot)$ is a ring.*

Proof. Let $a_1, b_1, a_2, b_2 \in Z_n$ such that $a_1 = b_1$ and $a_2 = b_2$. Let $x_1 \in a_1$, $y_1 \in b_1$, $x_2 \in a_2$ and $y_2 \in b_2$. Then

$$a_1 + a_2 = \overline{x_1 + x_2} = \overline{y_1 + y_2} = b_1 + b_2$$

and

$$a_1 \cdot a_2 = \overline{x_1 \cdot x_2} = \overline{y_1 \cdot y_2} = b_1 \cdot b_2$$

so $+$ and $\cdot$ are well defined. Now let $a_3 \in Z_n$ such that $x_3 \in a_3$. Note that

$$a_1 + a_2 = \overline{x_1 + x_2} = \overline{x_2 + x_1} = a_2 + a_1$$

and

$$(a_1 + a_2) + a_3 = \overline{x_1 + x_2} + \overline{x_3} = \overline{x_1 + x_2 + x_3} = \overline{x_1} + \overline{x_2 + x_3} = a_1 + (a_2 + a_3).$$

Also let $0 = \overline{0}$ so we have

$$a_1 + 0 = \overline{x_1 + 0} = \overline{x_1} = a_1$$

and let $-a_1 = \overline{-x_1}$ so we have

$$a_1 + -a_1 = \overline{x_1 + -x_1} = \overline{0} = 0.$$

Now note that

$$a_1 \cdot a_2 = \overline{x_1 \cdot x_2} = \overline{x_2 \cdot x_1} = a_2 \cdot a_1$$

and

$$(a_1 \cdot a_2) \cdot a_3 = \overline{x_1 \cdot x_2} \cdot \overline{x_3} = \overline{x_1 \cdot x_2 \cdot x_3} = \overline{x_1} \cdot \overline{x_2 \cdot x_3} = a_1 \cdot (a_2 \cdot a_3).$$

Now let $1 = \overline{1}$ so we have

$$a_1 \cdot 1 = \overline{x_1 \cdot 1} = \overline{x_1} = a_1.$$

Finally we have

$$\begin{aligned} a_1 \cdot (a_2 + a_3) &= \overline{x_1} \cdot \overline{x_2 + x_3} \\ &= \overline{x_1 \cdot x_2 + x_1 \cdot x_3} \\ &= \overline{x_1 \cdot x_2} + \overline{x_1 \cdot x_3} \\ &= a_1 \cdot a_2 + a_1 \cdot a_3. \end{aligned}$$

So we've show additive commutativity, associativity, identity, inverse, multiplicative commutativity, associativity, identity and also distributivity so Z_n is a ring. $\square$

Exercise 6 *Solve the following congruencies:*
1) $2x + 1 \equiv 3 \pmod 5$*;*
2) $x^2 \equiv 1 \pmod{17}$*;*
3) $2x \equiv 5 \pmod 8$*;*
4) $3x \equiv 3 \pmod 6$*.*

Definition 7 *Let R be a ring. An element $0 \neq a \in R$ is a zero divisor if there exists $0 \neq b \in R$ with $ab = 0$.*

Exercise 8 *What are the zero divisors modulo 6, 7 and 12?*

The zero divisors of 6 are 2 and 3. Since 7 is prime is has no zero divisors. The zero divisors of 12 are 2, 3, 4 and 6.

Lemma 9 *Let $0 \neq a \in R$ be a non-zero-divisor. Then $ax = ay$ implies $x = y$.*

Proof. We have $a(x - y) = ax - ay = 0$. But a is not a zero divisor so for all $0 \neq b \in R$ we have $ab \neq 0$. Therefore $(x - y) = 0$ and so $x = y$. $\square$

Theorem 10 *Let R be a finite ring. Then $0 \neq a \in R$ has a multiplicative inverse if and only if a is not a zero divisor.*

Proof. Suppose that a is not a zero divisor. Then for all $0 \neq b \in R$ we have $ab \neq 0$. Multiply a by every element of R which is not a zero divisor. Note that Lemma 9 implies that this is an injective process and so it must return every element which is not a zero divisor. But 1 is not a zero divisor and so there must exist $b \in R$ such that $ab = 1$.

Conversely assume that $0 \neq a \in R$ has a multiplicative inverse, b. Then $ab = 1$. If a is a zero divisor then there exists $0 \neq c \in R$ such that $ac = 0$. Then $a(b + c) = ab + ac = 1$ but then $b + c$ is a multiplicative inverse of a and since multiplicative inverses are unique, $b + c = b$ and $c \neq 0$. This is a contradiction and so a is a zero divisor. $\square$

Definition 11 *For a prime p let $\mathbb{F}_p = Z_p$.*

Theorem 12 *For a prime p every nonzero element of $\mathbb{F}_p$ is invertible.*

Proof. Let $0 \neq a \in \mathbb{F}_p$. Suppose there exists $0 \neq b \in \mathbb{F}_p$ such that $ab = 0$. Then $p \mid ab$ and so there exists $c \in \mathbb{Z}$ such that $pc = ab$. But then because of unique factorization we have $p \mid a$ or $p \mid b$. Thus either $a = 0$ or $b = 0$ which is a contradiction. Thus a is not a zero divisor and so it has a multiplicative inverse (20.10). $\square$

Theorem 13 (Wilson's Theorem) *Let p be a prime. Then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Since p is prime, every term in $(p-2)!$ is invertible in the field $\mathbb{F}_p$ (20.12). Note that 1 has its own inverse and for $p > 2$ we have $p - 3$ terms with inverses in the product $(p-2)!$ that aren't 1. Each of these pairs will multiply to 1 and 1 will multiply with that and so we're left with just $p - 1 \equiv -1 \pmod{p}$. $\square$

Theorem 14 *For all $a, b \in \mathbf{F}_p$ we have*

$$(a+b)^p = a^p + b^p.$$

Proof. We have

$$(a+b)^p = \sum_{k=1}^{p} \binom{p}{k} a^k b^{p-k} = \sum_{k=1}^{p} \frac{p!}{k!(p-k)!} a^k b^{p-k}$$

and each term of this sum will be 0 unless $k = 0$ or $k = p$ because of the $p!$ term. Thus we have

$$(a+b)^p = a^p + b^p.$$

$\square$

Theorem 15 (Fermat's Little Theorem) *Let p be a prime and let a be an integer. Then*

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

Proof. Note that if $p \mid a$ then we are done so assume that a is not a multiple of p. Consider the product

$$a^{p-1}(p-1)! \equiv \prod_{i=1}^{p-1} ia \equiv (p-1)! \pmod{p}$$

since a is not a zero divisor using the same injective logic as in Theorem 10 (20.10, 20.12). But then we have

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

and so

$$a^p = a$$

since a is not a zero divisor. □

Corollary 16 *Let p be a prime and let a be an integer not divisible by p. Then*

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

Proof. This follows from Theorem 15 (20.15). □

Theorem 17 *Let R be a finite ring and let $a \in R$ be invertible. Then there exists a natural number k with $a^k = 1$.*

Proof. Note that R is a finite ring and so there must exist $k, l \in \mathbb{N}$ with $k \neq l$ such that $a^k = a^l$. Without loss of generality assume that $k > l$. But then $k - l \in \mathbb{N}$ and since a is invertible, it's not a zero divisor (20.10). Then a^l is not a zero divisor as well. Thus $a^l = a^k = a^k a^{-l} a^l = a^{k-l} a^l$ implies $a^{k-l} = 1$ (20.9). □

Definition 18 *The minimal n with the above property is called the multiplicative order of a. We denote it by $o(a)$.*

Theorem 19 *Let $0 \neq a \in \mathbb{F}_p$. Then $o(a)$ divides $p - 1$.*

Proof. Note that $a^{o(a)} = a^{p-1}$ and since $o(a) \leq p - 1$ by definition we have $a^{\frac{p-1}{o(a)}} = 1$ so $o(a) \mid p - 1$. □

Theorem 20 *Let a be an integer and let n be a natural number. Then the following are equivalent:*
1) a is relatively prime to n;
2) a is invertible modulo n;
3) There exist integers x, y with $ax + ny = 1$.

Proof. Let a be relatively prime to n. Then a and n share no common factors and so for all $0 \neq b \in Z_n$ we have $ab \neq 0$. Thus a is not a zero divisor and so it must be invertible modulo n (20.10). Now assume that a is invertible modulo n. Then there exists x such that $ax = 1 \pmod n$ which means that there exists $y \in \mathbb{Z}$ such that $ny = 1 - ax$ and so $ax + ny = 1$. Finally assume that there exists integers x and y such that $ax + ny = 1$. Then $ny = 1 - ax$ and since ny and ax differ by a factor of 1 they share no common factors and so n and a are relatively prime. □

Definition 21 (Euler's Totient Function) *For a natural number n let $U(n)$ denote the set of invertible elements of Z_n. Let $\phi(n)$ be the size of $U(n)$.*

Exercise 22 *Find a formula for $\phi(n)$.*

Lemma 23 *If $a, b \in U(n)$ then $ab \in U(n)$.*

Proof. Since $a, b \in U(n)$ there exist $a^{-1}, b^{-1} \in Z_n$. Then take $a^{-1}b^{-1} \in Z_n$ and note that $ab \cdot a^{-1}b^{-1} = 1$. Thus $ab \in U(n)$. □

Theorem 24 *Let $0 \neq a \in Z_n$ be invertible. Then $o(a)$ divides $\phi(n)$.*

Theorem 25 (Euler's Theorem) *Let n be a natural number and let a be an integer relatively prime to n. Then*

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

Proof. Since a is relatively prime to n we have a is invertible modulo n (20.20). Then since $o(a) \mid \phi(n)$ we have

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

using Theorem 24 (20.24). □

Definition 26 *Complex numbers are* $\mathbb{R}[x]$ *modulo* $x^2 + 1$.