Лекция 2.1 по курсу

Математические основы криптологии

Университет ИТМО

Преподаватель: Петтай Павел Пээтерович

3. Сравнение по модулю. Свойства сравнений.

Выберем и зафиксируем некоторое *натуральное* число m и будем называть его *модулем сравнения*.

Опр.3.1. Говорят, что число a *сравнимо с числом* b *по модулю* m и пишут $a \equiv b \pmod m$, если $a - b \vdots m$.

Таким образом, $\boxed{a \equiv b \pmod m \Leftrightarrow a - b \vdots m}$.

Пример 3.1. $17 \equiv 5 \pmod 4$, т.к. $17 - 5 = 12 = 4 \cdot 3 \vdots 4$.

Пример 3.2. $17 \equiv 1 \pmod 4$, т.к. $17 - 1 = 16 = 4 \cdot 4 \vdots 4$.

Изучим и докажем некоторые простейшие свойства сравнений.

Свойство 3.1. (рефлексивность). $\boxed{a \equiv a \pmod m}$.

Доказательство. $a - a = 0 = m \cdot 0 \vdots m$. **Ч.т.д.**

Свойство 3.2. (симметричность). $\boxed{a \equiv b \pmod m \Leftrightarrow b \equiv a \pmod m}$.

Доказательство.
$a \equiv b \pmod m \Leftrightarrow a - b \vdots m \Leftrightarrow \exists k\ a - b = mk \Leftrightarrow b - a = -(mk) \Leftrightarrow b - a = m \cdot (-k) \Rightarrow$
$\Rightarrow b - a \vdots m \Leftrightarrow b \equiv a \pmod m$. **Ч.т.д.**

Свойство 3.3. (транзитивность).
$\boxed{a \equiv b \pmod m \wedge b \equiv c \pmod m \Rightarrow a \equiv c \pmod m}$

Пример 3.3. $15 \equiv 3 \pmod 4$, $3 \equiv -5 \pmod 4$, значит $15 \equiv -5 \pmod 4$

Доказательство. $a \equiv b \pmod m \Leftrightarrow a - b \vdots m$, $b \equiv c \pmod m \Leftrightarrow b - c \vdots m$. Тогда по Свойству 1.5. $a - c = (a - b) + (b - c) \vdots m \Leftrightarrow a \equiv c \pmod m$. **Ч.т.д.**

Свойство 3.4. $\boxed{a \equiv b \pmod{km} \Rightarrow a \equiv b \pmod m}$.

Доказательство.
$a \equiv b \pmod{km} \Leftrightarrow a - b \vdots km \Leftrightarrow \exists l\ a - b = km \cdot l \Leftrightarrow a - b = m \cdot (kl) \Rightarrow a - b \vdots m \Leftrightarrow$
$\Leftrightarrow a \equiv b \pmod m$ **Ч.т.д.**

Замечание 3.1. Обратное, разумеется, не верно. Так, например, $17 \equiv 11 \pmod 3$, но при этом $17 \not\equiv 11 \pmod{3 \cdot 4}$

Свойство 3.5. $\boxed{a \equiv b \pmod m \Leftrightarrow a + c \equiv b + c \pmod m}$.

Доказательство. $(a + c) - (b + c) = a - b \vdots m$. **Ч.т.д.**

<u>Свойство 3.6</u>. $\boxed{a \equiv b \pmod{m} \Rightarrow a \cdot c \equiv b \cdot c \pmod{m}}$.

Доказательство. По Свойству 1.2 $a \cdot c - b \cdot c = (a-b) \cdot c \,\vdots\, m$, т.к. $a - b \,\vdots\, m$. **Ч.т.д.**

Замечание 3.2. <u>Обратное не верно!</u> $\boxed{a \cdot c \equiv b \cdot c \pmod{m} \not\Rightarrow a \equiv b \pmod{m}}$. Например, $5 \cdot 12 \equiv 3 \cdot 12 \pmod{4}$ (т.к. $60 - 36 = 24 \,\vdots\, 4$), но $5 \not\equiv 3 \pmod{4}$, т.к. $5 - 3 = 2 \not\vdots\, 4$.

<u>Свойство 3.7</u>. $\boxed{a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}}$

Доказательство. $(a+c) - (b+d) = a + c - b - d = (a-b) + (c-d) \,\vdots\, m$. **Ч.т.д.**

Пример 3.4. $12 \equiv 2 \pmod{5}$ и $18 \equiv 3 \pmod{5}$, следовательно, $12 + 18 \equiv 2 + 3 \pmod{5}$, т.е. $30 \equiv 5 \pmod{5}$.

Замечание 3.3. Обратное, разумеется, не верно. Так, например, $12 + 18 \equiv 1 + 4 \pmod{5}$, но при этом $12 \not\equiv 1 \pmod{5}$ и $12 \not\equiv 4 \pmod{5}$.

<u>Следствие</u>. $\boxed{\forall k \in \{1, 2, ..., n\}\ a_k \equiv b_k \pmod{m} \Rightarrow \sum_{k=1}^{n} a_k \equiv \sum_{k=1}^{n} b_k \pmod{m}}$

Доказательство. Будем доказывать индукцией по n. При $n = 1$ утверждение очевидно. Если для некоторого n $\sum_{k=1}^{n} a_k \equiv \sum_{k=1}^{n} b_k \pmod{m}$, то по Свойству 3.7.,

$$\sum_{k=1}^{n} a_k \equiv \sum_{k=1}^{n} b_k \pmod{m} \wedge a_{n+1} \equiv b_{n+1} \pmod{m} \Rightarrow \sum_{k=1}^{n} a_k + a_{n+1} \equiv \sum_{k=1}^{n} b_k + b_{n+1} \pmod{m} \Leftrightarrow$$

$$\sum_{k=1}^{n+1} a_k \equiv \sum_{k=1}^{n+1} b_k \pmod{m}.$$ **Ч.т.д.**

<u>Свойство 3.8</u>. $\boxed{a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a - c \equiv b - d \pmod{m}}$

Доказательство. $(a-c) - (b-d) = a - c - b + d = (a-b) - (c-d) \,\vdots\, m$. **Ч.т.д**

<u>Свойство 3.9</u>. $\boxed{a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}}$

Доказательство. $ac - bd = ac - bc + bc - bd = (a-b)c + b(c-d) \,\vdots\, m$ (воспользовались Свойствами 1.2. и 1.5). **Ч.т.д.**

Пример 3.5. $12 \equiv 2 \pmod{5}$ и $18 \equiv 3 \pmod{5}$, следовательно, $12 \cdot 18 \equiv 2 \cdot 3 \pmod{5}$, т.е. $216 \equiv 6 \pmod{5}$.

Замечание 3.4. Обратное не верно! $\boxed{a\cdot c\equiv b\cdot d \pmod m \not\Rightarrow a\equiv b \pmod m \wedge c\equiv d \pmod m}$.

Например, $14\cdot 5\equiv 7\cdot 2 \pmod 8$, но $14\not\equiv 7 \pmod 8$ и $5\not\equiv 2 \pmod 8$, и $14\not\equiv 2 \pmod 8$, и $5\not\equiv 7 \pmod 8$.

Следствие. $\boxed{\forall k\in\{1,2,...,n\}\ a_k\equiv b_k \pmod m \Rightarrow \prod_{k=1}^{n} a_k \equiv \prod_{k=1}^{n} b_k \pmod m}$

Доказательство. Будем доказывать индукцией по n. При $n=1$ утверждение очевидно. Если для некоторого n $\prod_{k=1}^{n} a_k \equiv \prod_{k=1}^{n} b_k \pmod m$, то по Свойству 3.9.,

$$\prod_{k=1}^{n} a_k \equiv \prod_{k=1}^{n} b_k \pmod m \wedge a_{n+1}\equiv b_{n+1} \pmod m \Rightarrow (\prod_{k=1}^{n} a_k)\cdot a_{n+1} \equiv (\prod_{k=1}^{n} b_k)\cdot b_{n+1} \pmod m$$

$$\Leftrightarrow \prod_{k=1}^{n+1} a_k \equiv \prod_{k=1}^{n+1} b_k \pmod m.$$ **Ч.т.д.**

Свойство 3.10. $\boxed{\forall n\in\mathbb{N}\ a\equiv b \pmod m \Rightarrow a^n\equiv b^n \pmod m}$.

Доказательство. Будем доказывать индукцией по n. Для $n=1$ утверждение очевидно. Если для какого-нибудь $n\in\mathbb{N}$ $a^n\equiv b^n \pmod m$, то по Свойству 3.9.,

$$a\equiv b \pmod m \wedge a^n\equiv b^n \pmod m \Rightarrow a\cdot a^n\equiv b\cdot b^n \pmod m \Leftrightarrow a^{n+1}\equiv b^{n+1} \pmod m.$$

Ч.т.д.

То же самое можно было получить сразу: достаточно было n раз записать сравнение $a\equiv b \pmod m$ и воспользоваться Следствием Свойства 3.9.

Пример 3.6. $15\equiv -1 \pmod 4$, следовательно, $15^{100}\equiv(-1)^{100}=1 \pmod 4$, т.е. доказали, что $15^{100}-1 ⋮ 4$.

Замечание 3.5. Обратное не верно! $\boxed{a^n\equiv b^n \pmod m \not\Rightarrow a\equiv b \pmod m}$.

Например, $5^2\equiv 1^2 \pmod 8$, но $5\not\equiv 1 \pmod 8$ и $5\not\equiv -1 \pmod 8$.

Свойство 3.11. $\boxed{a\equiv b+c \pmod m \Leftrightarrow a-c\equiv b \pmod m}$, *т.е., как в уравнениях и неравенствах, слагаемые и вычитаемые можно переносить из одной стороны сравнения в другую со сменой знака.*

Доказательство.

$$a\equiv b+c \pmod m \overset{Св.3.5}{\Leftrightarrow} a+(-c)\equiv b+c+(-c) \pmod m \Leftrightarrow a-c\equiv b \pmod m.$$ **Ч.т.д.**

Свойство 3.12. $\boxed{f \in \mathbb{Z}[x] \wedge a \equiv b \pmod m \Rightarrow f(a) \equiv f(b) \pmod m}$, т.е., *если* f - *полином с целыми коэффициентами, то значения этого полинома в точках, сравнимых по модулю* m *сами сравнимы по модулю* m.

Доказательство. Пусть $f(x) = \sum_{k=0}^{n} c_k x^k$, где $\forall k\ c_k \in \mathbb{Z}$. Тогда $\forall k \in \{0,1,..,n\}$ $a \equiv b \pmod m \overset{Св.3.10.}{\Rightarrow} a^k \equiv b^k \pmod m \overset{Св.3.6.}{\Rightarrow} c_k a^k \equiv c_k b^k \pmod m \overset{Сл.Св.3.7.}{\Rightarrow}$ $\overset{Сл.Св.3.7.}{\Rightarrow} \sum_{k=0}^{n} c_k a^k \equiv \sum_{k=0}^{n} c_k b^k \pmod m \Leftrightarrow f(a) \equiv f(b) \pmod m$. **Ч.т.д.**

Свойство 3.13. *Любое число сравнимо по модулю с остатком от деления данного числа на модуль сравнения. Т.е., если* $a = mq + r$ *- деление с остатком, то* $a \equiv r \pmod m$.

Доказательство. $a = mq + r \Leftrightarrow a - r = mq \vdots m \Leftrightarrow a \equiv r \pmod m$. **Ч.т.д.**

Замечание 3.6. Из доказательства видно, что тот факт, что r - именно остаток от деления a на m никак не использовался, важно лишь, представление $a = mq + r$. Таким образом, $\boxed{a = mq + r \Leftrightarrow a \equiv r \pmod m}$.

4. Модулярная арифметика.

Для начала поймём, как устроено множество всех чисел, сравнимых с числом a по некоторому модулю m.

Утверждение 4.1. *Множество всех чисел, сравнимых с числом* a *по модулю* m *имеет вид* $\boxed{\{a + k \cdot m \mid k \in \mathbb{Z}\}}$.

Доказательство. $(a + km) - a = km \vdots m$, таким образом, каждое число из множества $\{a + k \cdot m \mid k \in \mathbb{Z}\}$ сравнимо с a по модулю m.

Теперь покажем, что любое число, сравнимое с a по модулю m, лежит в множестве $\{a + k \cdot m \mid k \in \mathbb{Z}\}$. Пусть $a_1 \equiv a \pmod m$, т.е. $a_1 - a \vdots m$, т.е. найдётся такое число l, что $a_1 - a = ml$, а значит $a_1 = a + ml \in \{a + k \cdot m \mid k \in \mathbb{Z}\}$. **Ч.т.д.**

Вспомним, что бинарные отношения, являющиеся одновременно рефлексивными, симметричными и транзитивными называют *отношениями эквивалентности*. Таким образом, из Свойств 3.1-3.3. следует, что *отношение сравнимости чисел по модулю является отношением эквивалентности*.

Любое отношение эквивалентности разбивает всё множество, на котором задано отношение, на непересекающиеся классы эквивалентности.

Опр.4.1. *Классом вычетов по модулю* m*, содержащим элемент* a называется множество всех элементов, сравнимых с элементом a по модулю m и обозначается $[a]_m$. В этом случае сам элемент a называют также *представителем класса* $[a]_m$.

Таким образом, $\boxed{[a]_m = \{a + k \cdot m \mid k \in \mathbb{Z}\}}$.

Опр.4.2. Каждый элемент класса вычетов называют *вычетом*.

Например, $[2]_5 = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$

Множество всех классов вычетов по модулю m обозначают $\mathbb{Z} / m\mathbb{Z}$.

<u>Утверждение 4.2</u>. *Каждый класс вычетов однозначно задаётся модулем сравнения и любым своим элементом*, т.е. $\boxed{b \in [a]_m \Rightarrow [b]_m = [a]_m}$.

Доказательство. $b \in [a]_m \Rightarrow \exists l : b = a + ml$. Пусть $c \in [b]_m \Rightarrow \exists t : c = b + mt$, но тогда $c = b + mt = (a + ml) + mt = a + m(l + t) \Rightarrow c \in [a]_m$. В силу произвольности выбора c заключаем, что $[b]_m \subseteq [a]_m$. Обратно, пусть $d \in [a]_m \Rightarrow \exists u : d = a + mu$, тогда $d = a + mu = (b - ml) + mu = b + m(u - l) \Rightarrow d \in [b]_m$. В силу произвольности выбора d заключаем, что $[a]_m \subseteq [b]_m$ и значит $[b]_m = [a]_m$.

Ч.т.д.

<u>Утверждение 4.3</u>. *Разные остатки при делении на* m *расположены в разных классах вычетов по модулю* m.

Доказательство. По определению любой класс вычетов состоит из элементов, сравнимых по модулю m, т.е. разность любых двух элементов одного класса кратна m. $\{0, 1, \ldots, m-1\}$ - множество всех возможных остатков при делении на m. Легко видеть, что модуль разности любых двух элементов этого множества строго меньше m и по Свойству 1.7. может делиться на m лишь в том случае, когда равен нулю, но в этом случае остатки совпадают. **Ч.т.д.**

<u>Теорема 4.1</u>. *Существует ровно* m *разных классов вычетов по модулю* m. *Эти классы могут быть заданы, как* $\boxed{[0]_m, [1]_m, \ldots, [m-1]_m}$.

Доказательство. Есть ровно m разных остатков при делении m: $0, 1, \ldots, m-1$, согласно Свойству 1.3., каждое целое число сравнимо с одним из них по модулю m, т.е. принадлежит одному из классов: $[0]_m, [1]_m, \ldots, [m-1]_m$, а в силу Утверждения 4.3. все эти классы различны. Наконец, в силу Утверждения 4.2., класс вычетов, порождённый любым числом класса $[i]_m$ совпадает с самим классом $[i]_m$ для всех i от 0 до $m-1$. **Ч.т.д.**

Пример 4.1. Найдём множество всех чисел, с которыми сравнимо число 122 по модулю 7.

Решение. $122 = 7 \cdot 17 + 3$, т.е. 122 имеет остаток 3 при делении на 7, следовательно $122 \equiv 3 \pmod 7$ и тогда искомое множество имеет вид $\{3 + 7k \mid k \in \mathbb{Z}\}$. Например, при $k = 101$ получим $3 + 7 \cdot 101 = 710$, т.е. сразу можем утверждать, что $122 \equiv 710 \pmod 7$.

Опр.4.3. Совокупность m чисел, содержащая по одному представителю из каждого класса вычетов по модулю m, образуют *полную систему вычетов по модулю* m.

Пример 4.2. Полной системой вычетов по модулю 3 будет $\{-16, 42, 13\}$. Действительно, в силу Теоремы 4.1, $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$, в свою очередь, $-16 \equiv 2 \pmod 3$, т.е. $-16 \in [2]_3$, $42 \equiv 0 \pmod 3$, т.е. $42 \in [0]_3$, $13 \equiv 1 \pmod 3$, т.е. $13 \in [1]_3$.

Опр.4.3. Множество $\{0, 1, ..., m-1\}$ называют *системой наименьших неотрицательных вычетов по модулю* m.

Вычеты часто приходится возводить в большие степени, в свою очередь, возведение в степень меньших по модулю чисел может потребовать меньше вычислений. Особенно удобно возводить в степень числа, равные по модулю, но отличающиеся знаком (если возвели одно, то в одно действие можем возвести и другое).

Утверждение 4.4. *Любые m подряд идущих целых чисел образуют полную систему вычетов по модулю m.*

Доказательство. Согласно Свойству 1.9, среди любых m подряд идущих целых чисел ровно одно кратно m, т.е. сравнимо с нулём по модулю m. Пусть это число x из рассматриваемого набора. Тогда, если в данном наборе есть также числа $x+1, x+2, ..., x+k$, то, Согласно Свойству 3.5., они будут сравнимы с $1, 2, ..., k$ соответственно по модулю m. Если в наборе есть также числа $x-1, x-2, ..., x-l$, то, Согласно Свойству 3.5., они будут сравнимы с $-1, -2, ..., -l$ соответственно по модулю m. Очевидно, что $-i \equiv m - i \pmod m$, поэтому числа $-1, -2, ..., -l$ сравнимы с $m-1, m-2, ..., m-l$ по модулю m. Т.к. по условию числа идут подряд, $l + 1 + k = m \Leftrightarrow m - l = k + 1$. Таким образом, по модулю m числа исходного набора сравнимы, соответственно, с числами $m-1, m-2, ..., k+1, 0, 1, ..., k$, с точностью до порядка элементов, это и есть $0, 1, ..., m-1$. **Ч.т.д.**

Например, числа $117, 118, 119, 120, 121$ образуют полную систему вычетов по модулю 5. Действительно, если договориться операцию сравнения применять к упорядоченным наборам поэлементно, то получим, что $(117, 118, 119, 120, 121) \equiv (-3, -2, -1, 0, 1) \equiv (2, 3, 4, 0, 1) \pmod 5$.

Опр.4.4. *Системой абсолютно наименьших вычетов по модулю* m называют $\left\{-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}\right\}$ при нечётных m и $\left\{-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2}\right\}$ при чётных m.

Идея в том, чтобы сдвинуть систему наименьших неотрицательных вычетов так, чтобы расположить 0 максимально близко к центру. В силу Утверждения 4.4., полученный набор, по-прежнему, останется полной системой вычетов.

Пример 4.3. Системой абсолютно наименьших вычетов по модулю 5 будет $\{-2, -1, 0, 1, 2\}$.

Пример 4.4. Системой абсолютно наименьших вычетов по модулю 8 будет $\{-3, -2, -1, 0, 1, 2, 3, 4\}$.

Будем обозначать $\boxed{\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}}$.

Естественным образом, введём над элементами $\mathbb{Z}_m$ бинарные операции «сложения» $\oplus$ и «умножения» $\odot$:

- $\boxed{\forall\, [a]_m, [b]_m \in \mathbb{Z}_m\ [a]_m \oplus [b]_m = [a+b]_m}$
- $\boxed{\forall\, [a]_m, [b]_m \in \mathbb{Z}_m\ [a]_m \odot [b]_m = [a \cdot b]_m}$

Для этих операций специально использованы «нестандартные» обозначения, чтобы подчеркнуть, что речь идёт об *операциях с классами вычетов*, а не с числами, являющимися элементами классов вычетов.

Опираясь на них, мы можем также естественно ввести унарные операции взятия противоположного элемента и возведения в натуральную степень, бинарную операцию вычитания.

- $\boxed{\forall\, [a]_m \in \mathbb{Z}_m\ -[a]_m = [-a]_m}$
- $\boxed{\forall\, [a]_m \in \mathbb{Z}_m\ \forall n \in \mathbb{N}\ [a]_m{}^n = [a^n]_m}$
- $\boxed{\forall\, [a]_m, [b]_m \in \mathbb{Z}_m\ [a]_m - [b]_m = [a-b]_m}$

Нам нужно показать, что введённые операции являются корректными. Например, по определению, $[5]_{11} \oplus [8]_{11} = [5+8]_{11}$. В свою очередь, $[5]_{11} = [27]_{11}$,

$[8]_{11} = [-3]_{11}$ и $[27]_{11} \oplus [-3]_{11} = [27 + (-3)]_{11}$. Возникает вопрос, верно ли, что $[5+8]_{11} = [27 + (-3)]_{11}$? Если бы ответ был отрицательным, это говорило бы о некорректности введения операций таким образом.

Утверждение 4.5. *Введённые операции над классами вычетов являются корректными.*

Доказательство. Ясно, что, если $a, b \in \{0,1,...,m-1\}$, то совершенно не обязательно $a + b \in \{0,1,...,m-1\}$ и уж точно $\forall a\ a \neq 0 \rightarrow -a \notin \{0,1,...,m-1\}$. Однако это и не нужно, т.к., согласно Теореме 4.1, и $a+b$, и $-a$ точно попадают в один из классов вычетов $[0]_m, [1]_m, ..., [m-1]_m$. Таким образом, введённые операции не выводят из множества $\mathbb{Z}_m$.

Теперь обоснуем единственность, иными словами, нам *нужно доказать, что результат операции не зависит от выбора порождающих элементов классов*.

Пусть $x \in [a]_m, y \in [b]_m$, тогда $x \equiv a \pmod m$, $y \equiv b \pmod m$ и по Свойству 3.7. $x + y \equiv a + b \pmod m$, а значит, $[x+y]_m = [a+b]_m$. Так же, по Свойству 3.9. $x \cdot y \equiv a \cdot b \pmod m$, а значит, $[x \cdot y]_m = [a \cdot b]_m$. По Свойству 3.6., $x \equiv a \pmod m \Leftrightarrow -x \equiv -a \pmod m$, а значит, $[-x]_m = [-a]_m$. По Свойству 3.10., $x \equiv a \pmod m \Leftrightarrow x^n \equiv a^n \pmod m$, а значит, $[x^n]_m = [a^n]_m$. Наконец, по Свойству 3.8., $x - y \equiv a - b \pmod m$, а значит, $[x-y]_m = [a-b]_m$. **Ч.т.д.**

Теорема 4.2. *Алгебраическая структура* $< \mathbb{Z}_m, \oplus, \odot >$ *образует коммутативное кольцо с единицей.*

Доказательство. Нам нужно доказать выполнение восьми свойств целых чисел, которые без доказательства были перечислены в самом начале нашего курса. При этом уже известные нам свойства целых чисел будут самым непосредственным образом использоваться в доказательствах.

1. Коммутативность сложения:

$$[a]_m \oplus [b]_m = [a+b]_m = [b+a]_m = [b]_m \oplus [a]_m$$

2. Ассоциативность сложения:

$$([a]_m \oplus [b]_m) \oplus [c]_m = [a+b]_m \oplus [c]_m = [(a+b)+c]_m = [a+(b+c)]_m =$$
$$= [a]_m \oplus [b+c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$$

3. Существование нейтрального элемента по сложению (нуля):

$$[0]_m \oplus [a]_m = [a]_m \oplus [0]_m = [a+0]_m = [a]_m$$

4. Существование противоположного элемента (обратного по сложению):

$$[-a]_m \oplus [a]_m = [a]_m \oplus [-a]_m = [a+(-a)]_m = [0]_m$$

5. Коммутативность умножения:

$$[a]_m \odot [b]_m = [a \cdot b]_m = [b \cdot a]_m = [b]_m \odot [a]_m$$

6. Ассоциативность сложения:

$$([a]_m \odot [b]_m) \odot [c]_m = [a \cdot b]_m \odot [c]_m = [(a \cdot b) \cdot c]_m = [a \cdot (b \cdot c)]_m =$$
$$= [a]_m \odot [b \cdot c]_m = [a]_m \odot ([b]_m \odot [c]_m)$$

7. Существование нейтрального элемента по умножению (единицы):

$$[1]_m \odot [a]_m = [a]_m \odot [1]_m = [a \cdot 1]_m = [a]_m$$

8. Дистрибутивность умножения относительно сложения:

$$([a]_m \oplus [b]_m) \odot [c]_m = [a+b]_m \odot [c]_m = [(a+b) \cdot c]_m = [a \cdot c + (b \cdot c)]_m =$$
$$= [a \cdot c]_m \oplus [b \cdot c]_m = ([a]_m \odot [c]_m) \oplus ([b]_m \odot [c]_m)$$

$$[c]_m \odot ([a]_m \oplus [b]_m) = ([a]_m \oplus [b]_m) \odot [c]_m = ([a]_m \odot [c]_m) \oplus ([b]_m \odot [c]_m) =$$
$= ([c]_m \odot [a]_m) \oplus ([c]_m \odot [b]_m)$. **Ч.т.д.**

Из того, что $\mathbb{Z}_m$ - коммутативное кольцо с единицей, следует, что в нём выполнены свойства, аналогичные свойствам 9-15 для операций на множестве целых чисел $\mathbb{Z}$. С точностью до обозначений (замены a на $[a]_m$, операции + на операцию $\oplus$ и т.п.), доказательства *полностью* совпадают с доказательством соответствующих свойств на $\mathbb{Z}$. Ещё легче можно привести доказательства, построенные по аналогии с доказательством Теоремы 4.2, опирающиеся на уже известные нам свойства 9-15 для целых чисел. Потому оставим доказательства читателю в качестве несложного упражнения.

Утверждение 4.6. *Операции на множестве $\mathbb{Z}_m$ обладают следующими свойствами:*

- $\boxed{\forall a \in \mathbb{Z}\, [a]_m \odot [0]_m = [0]_m \odot [a]_m = [0]_m}$
- $\boxed{\forall a \in \mathbb{Z}\, [-1]_m \odot [a]_m = [a]_m \odot [-1]_m = [-a]_m}$
- $\boxed{\forall a \in \mathbb{Z}\, -(-[a]_m) = [a]_m}$
- $\boxed{[-1]_m \odot [-1]_m = [1]_m}$
- $\boxed{\forall a,b \in \mathbb{Z}\, [-a]_m \odot [-b]_m = [a \cdot b]_m}$
- $\boxed{\forall a,b \in \mathbb{Z}\, [a]_m \odot [-b]_m = [-a]_m \odot [b]_m = -[a \cdot b]_m}$

- $\boxed{\forall a,b,c\in\mathbb{Z}\ \ [a]_m\odot([b]_m-[c]_m)=([a]_m\odot[b]_m)-([a]_m\odot[c]_m)}$ и
  $\boxed{\forall a,b,c\in\mathbb{Z}\ \ ([b]_m-[c]_m)\odot[a]_m=([b]_m\odot[a]_m)-([c]_m\odot[a]_m)}$

Привычными свойствами обладает и операция возведения в степень.

<u>**Утверждение 4.7**</u>**.** *Операция возведения в натуральную степень на множестве $\mathbb{Z}_m$ обладает следующими свойствами:*

- $\boxed{\forall a,b\in\mathbb{Z}\ \forall n\in\mathbb{N}\ [a]_m{}^n\odot[b]_m{}^n=([a]\odot[b]_m)^n}$
- $\boxed{\forall a\in\mathbb{Z}\ \forall k,n\in\mathbb{N}\ [a]_m{}^k\odot[a]_m{}^n=[a]_m{}^{k+n}}$
- $\boxed{\forall a\in\mathbb{Z}\ \forall k,n\in\mathbb{N}\ ([a]_m{}^k)^n=[a]_m{}^{k\cdot n}}$

Доказательство.
$[a]_m{}^n\odot[b]_m{}^n=[a^n]_m\odot[b^n]_m=[a^n\cdot b^n]_m=[(a\cdot b)^n]_m=[a\cdot b]_m{}^n=([a]\odot[b]_m)^n$
$[a]_m{}^k\odot[a]_m{}^n=[a^k]_m\odot[a^n]_m=[a^k\cdot a^n]_m=[a^{k+n}]_m=[a]_m{}^{k+n}$
$([a]_m{}^k)^n=([a^k]_m)^n=[(a^k)^n]_m=[a^{k\cdot n}]_m=[a]_m{}^{k\cdot n}$. **Ч.т.д.**

Мы доказали, что $<\mathbb{Z}_m,\oplus,\odot>$ является кольцом, но, может быть, есть возможность доказать большее и утверждать, что $<\mathbb{Z}_m,\oplus,\odot>$ - поле? Для этого необходимо доказать обратимость по умножению для всех ненулевых элементов кольца. Будем использовать стандартное обозначение $[a]_m{}^{-1}$ для элемента, обратного к элементу $[a]_m$ по умножению, т.е. такого, что $[a]_m{}^{-1}\odot[a]_m=[1]_m$. Проверим на примерах.

Пример 4.5. $\mathbb{Z}_3=\{[0]_3,[1]_3,[2]_3\}$. $[1]_3\odot[1]_3=[1]_3$, поэтому $[1]_3{}^{-1}=[1]_3$ (единица кольца всегда обратима, причём обратным элементом является она сама). $[2]_3\odot[2]_3=[2\cdot 2]_3=[4]_3=[1]_3$, поэтому $[2]_3{}^{-1}=[2]_3$. Таким образом, все ненулевые элементы $\mathbb{Z}_3$ обратимы по умножению, а значит $\mathbb{Z}_3$ - *поле*.

Пример 4.6. $\mathbb{Z}_4=\{[0]_4,[1]_4,[2]_4,[3]_4\}$. Аналогично $[1]_4{}^{-1}=[1]_4$ (единица кольца всегда обратима, причём обратным элементом является она сама). $[2]_4\odot[2]_4=[2\cdot 2]_4=[4]_4=[0]_4\neq[1]_4$, $[2]_4\odot[0]_4=[0]_4\neq[1]_4$,
$[2]_4\odot[1]_4=[2]_4\neq[1]_4$, наконец, $[2]_4\odot[3]_4=[2\cdot 3]_4=[6]_4=[2]_4\neq[1]_4$. Таким образом, класс $[2]_4$ не имеет обратного элемента, что говорит о том, что $\mathbb{Z}_4$ - *не поле*.

Замечание 4.1. Не сложно проверить, что $[3]_4{}^{-1}=[3]_4$, но это ничего не меняет.

Исследование (важного!) вопроса, в каких случаях $\mathbb{Z}_m$ образует поле будет произведено позднее после разработки необходимой теоретической базы.