Спецкурс

“Алгоритмическая теория чисел и элементы криптографии”

Лекция 1
Алгоритм Евклида

1.1. Теорема (Алгоритм Евклида). Пусть a и b – натуральные числа. Положим $a_0 = a$ и $a_1 = b$, и будем делить с остатком по указанной ниже схеме до тех пор, пока очередной остаток станет нулевым:

$$\begin{cases} a_0 = a_1 q_1 + a_2, & 0 < a_2 < a_1, \\ a_1 = a_2 q_2 + a_3, & 0 < a_3 < a_2, \\ \dots \\ a_{n-2} = a_{n-1} q_{n-1} + a_n, & 0 < a_n < a_{n-1}, \\ a_{n-1} = a_n q_n. \end{cases}$$

Тогда $a_n = \mathbf{нод}(a, b)$. Более того, найдутся целые числа u, v такие, что

$$ua + vb = \mathbf{нод}(a, b).$$

1.2. Следствие. Если a и n – взаимно простые числа, то существует такое число u, что $au \equiv 1 \pmod{n}$.

Определим числа Фибоначчи: $F_1 = F_2 = 1,\ \ F_{i+2} = F_{i+1} + F_i$.

1.3. Лемма. Если $n \geqslant 2$, то $F_{n+5} > 10F_n$.

Доказательство. $F_{n+5} = F_{n+4} + F_{n+3} = 2F_{n+3} + F_{n+2} = 3F_{n+2} + 2F_{n+1} = 5F_{n+1} + 3F_n = 8F_n + 5F_{n-1} > 8F_n + 4F_{n-1} \geqslant 8F_n + 2F_n = 10F_n$. Мы использовали то, что $F_n = F_{n-1} + F_{n-2} \leqslant 2F_{n-1}$. $\square$

1.4. Теорема Ламе. Пусть a и b – натуральные числа, $a > b > 0$. Тогда число делений в алгоритме Евклида не больше, чем $5k$, где k – число цифр в десятичной записи числа b.

Доказательство. Имеем, $a_n \geqslant 1 = F_2$ и $a_{n-1} > a_n \geqslant 1$. Тогда $a_{n-1} \geqslant 2 = F_3$. Далее, $a_{n-2} \geqslant a_{n-1} q_{n-1} + a_n \geqslant a_{n-1} + a_n \geqslant F_2 + F_3 = F_4$. Продолжая далее, получаем $b = a_1 \geqslant F_{n+1}$. Если $n > 5k$, то $b \geqslant F_{5k+2} > 10^k F_2 = 10^k$ – противоречие. $\square$

1.5. Упражнение. 1) Докажите, что F_{kl} делится на F_k. Тем самым будет доказано, что если F_n – простое, то n – простое или $n = 4$ (заметим, что $F_4 = 3$ делится на $F_2 = 1$).

2) Найти наименьшее простое $n > 2$ такое, что число F_n не простое.

Лекция 2
Структура кольца вычетов $\mathbb{Z}_m$

2.1. Пример. Рассмотрим пример сложения и умножения наименьших неотрицательных остатков по модулю 4:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Обозначим $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Прочитав определения в следующих пунктах, полезно понять что $\mathbb{Z}_4$ с операцией сложения образует группу, а с операцией умножения – нет. Кроме того, $\mathbb{Z}_4$ с обеими операциями образует кольцо.

2.2. Определение группы. Говорят, что на множестве G определена *бинарная операция* $\cdot$, если для любых двух элементов a и b из G определен элемент $a \cdot b$ из G. Бинарная операция может обозначаться не только $\cdot$, но и любым другим символом, например $+$. Обычно пишут ab вместо $a \cdot b$.

Непустое множество G с определенной на нем бинарной операцией называется *группой*, если

1) $(ab)c = a(bc)$ для любых элементов a, b из G (операция *ассоциативна*);

2) существует такой элемент e из G (он называется *единицей*), что $ae = ea = a$ для любого a из G;

3) для любого a из G существует такой элемент b из G (он называется *обратным* к a), что $ab = ba = e$.

Для обозначения единичного элемента используют также символ 1, если операция обозначается точкой, и символ 0, если операция обозначается плюсом.

Можно доказать, что единица в любой группе G единственна и для любого a из G существует только один обратный к a элемент.

Группа называется *абелевой* или *коммутативной*, если $ab = ba$ для любых a, b из G.

Группы G и G_1 называют *изоморфными*, если существует *изоморфизм* $\phi : G \to G_1$, то есть такое взаимно однозначное отображение ϕ из группы G на всю группу G_1, что $\phi(ab) = \phi(a)\phi(b)$ для любых a, b из G.

2.3. Определение кольца. Непустое множество K с определенными на нем бинарными операциями $+$ и $\cdot$ называется *кольцом*, если

1) K является абелевой группой относительно сложения, т. е. выполняются аксиомы:

а) $(a + b) + c = a + (b + c)$;

б) существует такой элемент $0 \in K$, что $a + 0 = 0 + a = a$ для любого a из K;

в) для любого $a \in K$ существует такой элемент $b \in K$, что $a + b = 0$;

г) $a + b = b + a$;

2) В K выполняются законы левой и правой дистрибутивности:

д) $a(b + c) = ab + ac$;

е) $(a + b)c = ab + ac$.

Кольцо называется *ассоциативным*, если $(ab)c = a(bc)$ $\forall a, b, c \in K$.

Кольцо называется *коммутативным*, если $ab = ba \ \forall a, b \in K$.

Элемент $b \in K$ называется *единицей* кольца K, если $ba = a = ab \ \forall a \in K$.

Можно доказать, что единица в кольце единственна, если существует. Единица кольца обозначается через 1.

Аддитивной группой кольца K называется группа, заданная на множестве K с помощью операции $+$, имеющейся в кольце. Такая группа обозначается K^+. Если же рассмотреть кольцо K только относительно умножения, то группы не получится. Однако, при дополнительных предположениях некоторая часть кольца K все же является группой относительно умножения. Пусть K – ассоциативное и комутативное кольцо с единицей. Обозначим через K^* множество тех элементов $a \in K$, для которых существует *обратный*, т. е. элемент $b \in K$ со свойством $ab = ba = 1$. Тогда K^* является группой относительно умножения и называется *мультипликативной группой кольца* K.

Кольца K и K_1 называют *изоморфными*, если существует *изоморфизм* $\phi : K \to K_1$, то есть такое взаимно однозначное отображение ϕ из кольца R на все кольцо K_1, что $\phi(a + b) = \phi(a) + \phi(b)$ и $\phi(ab) = \phi(a)\phi(b)$ для любых a, b из K.

2.4. Определение кольца вычетов $\mathbb{Z}_m$. Пусть x и m – натуральные числа. Обозначим через $\mathrm{rest}_m(x)$ наименьший неотрицательный остаток от деления x на m. Таким образом, $0 \leqslant \mathrm{rest}_m(x) \leqslant m - 1$ и разность $x - \mathrm{rest}_m(x)$ делится на m. Все возможные наименьшие неотрицательные остатки при делении натуральных чисел на m образуют множество

$$\mathbb{Z}_m = \{0, 1, \dots, m - 1\}.$$

Зададим на нем сложение и умножение правилами:

– сумма элементов i и j равна $\mathrm{rest}_m(i + j)$;

– произведение элементов i и j равно $\mathrm{rest}_m(i \cdot j)$.

Легко проверить, что $\mathbb{Z}_m$ становится кольцом. Оно называется *кольцом вычетов по модулю* m.

2.5. Определение прямой суммы колец. Пусть $K_1, \dots, K_s$ – некоторые кольца. Обозначим

$$K_1 \oplus \dots \oplus K_s = \{(r_1, \dots, r_s) \mid r_i \in K_i \ \forall i\}.$$

Введем на этом множестве операции сложения и умножения:

$$(r_1, \dots, r_s) + (r'_1, \dots, r'_s) = (r_1 + r'_1, \dots, r_s + r'_s),$$
$$(r_1, \dots, r_s) \cdot (r'_1, \dots, r'_s) = (r_1 \cdot r'_1, \dots, r_s \cdot r'_s).$$

Тогда легко проверить, что $K_1 \oplus \dots \oplus K_s$ становится кольцом. Это кольцо называется *прямой суммой* колец $K_1, \dots, K_s$.

Его нуль – это $(0, \dots, 0)$, его единица – это $(1, \dots, 1)$, если каждое K_i имеет единицу.

2.6. Теорема о разложении кольца $\mathbb{Z}_m$. Пусть $m = m_1 m_2 \dots m_s$, где все $m_i \in \mathbb{N}$ и попарно взаимно просты. Тогда $\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}$ как кольца.

Доказательство. Пусть $0 \leqslant x \leqslant m - 1$ – произвольный элемент $\mathbb{Z}_m$. Проверим, что правило

$$\phi : x \mapsto (\mathrm{rest}_{m_1}(x), \dots, \mathrm{rest}_{m_s}(x))$$

задает требуемый изоморфизм.

1) Проверим, что отображение ϕ взаимно однозначно. Предположим, что для некоторых $x, y \in \mathbb{Z}_m$ выполняется $\mathrm{rest}_{m_i}(x) = \mathrm{rest}_{m_i}(y)$ для всех i. Тогда $x - y$ делится

на m_i для всех i. Так как числа $m_1, \ldots, m_s$ попарно взаимно просты, то $x-y$ делится на их произведение m. Отсюда и из $0 \leqslant x, y \leqslant m-1$ следует $x = y$.

2) Проверим, что ϕ – отображение "на". Это непосредственно вытекает из того, что ϕ взаимно однозначно и, что число элементов в $\mathbb{Z}_m$ равно числу элементов в $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$.

3) Проверим, что $\phi(x+y) = \phi(x) + \phi(y)$. Это равенство равносильно тому, что для любого i выполняется $\mathrm{rest}_{m_i}(x+y) = \mathrm{rest}_{m_i}(\mathrm{rest}_{m_i}(x) + \mathrm{rest}_{m_i}(y))$. Последнее равенство выполняется в силу того, что $(x+y) - (\mathrm{rest}_{m_i}(x) + \mathrm{rest}_{m_i}(y))$ делится на m_i.

4) Аналогично проверяется, что $\phi(xy) = \phi(x)\phi(y)$. $\square$

Для выполнения обратного перехода от набора $(x_1, \ldots, x_s)$ к элементу x применяется китайская теорема об остатках.

2.7. Китайская теорема об остатках. Пусть $m = m_1 m_2 \ldots m_s$, где все $m_i \in \mathbb{N}$ и попарно взаимно просты, и пусть $(x_1, \ldots, x_s)$ – набор натуральных чисел. Тогда существует число x, дающее остатки $x_1, \ldots, x_s$ по модулям $m_1, \ldots, m_s$ соответственно. Одно из таких чисел находится по формуле

$$x_0 = \sum_{i=1}^{s} c_i (m/m_i) x_i,$$

где c_i – обратный к m/m_i в кольце $\mathbb{Z}_{m_i}$, т.е. $c_i(m/m_i) \equiv 1 \pmod{m_i}$. Все другие x сравнимы с x_0 по модулю m.

Доказательство. Заметим сначала, что m/m_i делится на m_j при $i \neq j$. Тогда по модулю m_j справедливо сравнение

$$c_i(m/m_i)x_i \equiv \begin{cases} 0 & \text{при} \;\; i \neq j \\ x_j & \text{при} \;\; i = j. \end{cases}$$

Отсюда $x_0 \equiv x_j \pmod{m_j}$ при $j = 1, \ldots, s$. Предположим, что x – другое число, дающее остатки $x_1, \ldots, x_s$ при делении на $m_1, \ldots, m_s$. Тогда $x - x_0 \equiv 0 \pmod{m_i}$ для всех i. Так как числа $m_1, \ldots, m_s$ попарно взаимно просты, то $x - x_0 \equiv 0 \pmod{m}$. $\square$

Лекция 3
Основные понятия теории групп

3.1. Определение циклической группы. Группа G называется *циклической*, если в ней существует элемент g такой, что любой элемент G является его степенью, т.е.

$$\forall x \in G\, \exists n \in \mathbb{Z} : x = g^n.$$

При этом пишут $G = \langle g \rangle$ и говорят, что G *порождается* элементом g, а сам g называют *порождающим*.

3.2. Пример. 1) $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\} = \langle 1 \rangle = \langle 5 \rangle$.

2) $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle = \langle 5 \rangle$.

Действительно, $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$, так как только к этим элементам кольца $\mathbb{Z}_9$ существуют обратные (они равны $1, 5, 7, 2, 4, 8$, соответственно). Кроме того, проверка показывает, что $\mathbb{Z}_9^* = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\}$ (напомним, что порядок элементов в множестве неважен). Это позволяет установить изоморфизм групп $\mathbb{Z}_6^+ \to \mathbb{Z}_9^*$ по правилу $i \mapsto 2^i$.

3) $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$.

Аналогично устанавливается изоморфизм $\mathbb{Z}_6^+ \to \mathbb{Z}_7^*$ по правилу $i \mapsto 3^i$.

4) Группа $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ не циклическая.

3.3. Определение порядка элемента группы. *Порядок элемента* g группы G – это наименьшее натуральное $n \geqslant 1$ такое, что $g^n = e$ в G при условии, что такое n существует. Если же такое n не существует, то порядок g полагают равным ∞. Порядок g обозначается через $\mathrm{ord}(g)$.

В частности, $\mathrm{ord}(e) = 1$. Легко понять, что порядок любого элемента конечной группы конечен.

3.4. Пример. 1) Группа $\mathbb{Z}^+$ всех целых чисел по сложению – циклическая, $\mathbb{Z}^+ = \langle 1 \rangle$ и $\mathrm{ord}(n) = \infty$ для любого $n \in \mathbb{Z}$, отличного от 0.

2) Порядки элементов групп $\mathbb{Z}_6^+, \mathbb{Z}_9^*$ и $\mathbb{Z}_8^*$ следующие:

g	0	1	2	3	4	5
$\mathrm{ord}(g)$	1	6	3	2	3	6

g	1	2	4	5	7	8
$\mathrm{ord}(g)$	1	6	3	6	3	2

g	1	3	5	7
$\mathrm{ord}(g)$	1	2	2	2

3.5. Основные утверждения о порядках элементов в группе.

(1) Если g – элемент группы, то $g^n = e$ выполняется тогда и только тогда, когда n делится на $\mathrm{ord}(g)$.

(2) Если G – абелева группа, и $a, b \in G$ – элементы взаимно простых порядков, то $\mathrm{ord}(ab) = \mathrm{ord}(a)\mathrm{ord}(b)$.

(3) Если $G = \langle g \rangle$ – конечная циклическая группа, то $G = \{e, g, g^2, \ldots, g^{\mathrm{ord}(g)-1}\}$ и все перечисленные элементы различны.

Доказательство. (1) Если n делится на $\mathrm{ord}(g)$, то $g^n = (g^{\mathrm{ord}(g)})^{n/\mathrm{ord}(g)} = e$. Наоборот, пусть $g^n = e$. Поделим n на $\mathrm{ord}(g)$ с остатком: $n = k \cdot \mathrm{ord}(g) + r$, где $0 \leqslant r < \mathrm{ord}(g)$. Тогда $e = g^n = (g^{\mathrm{ord}(g)})^k g^r = g^r$. Чтобы не получилось противоречия с минимальностью $\mathrm{ord}(g)$ необходимо $r = 0$. Таким образом, n делится на $\mathrm{ord}(g)$.

(2) Обозначим k =ord(ab), n =ord(a), m =ord(b). Пользуясь абелевостью группы G, выводим $e = (ab)^{km} = a^{km}(b^m)^k = a^{km}$. По утверждению (1), km делится на n. Так как m и n взаимно просты, то k делится на n. Аналогично k делится на m, и, значит, на nm. С другой стороны, очевидно, что $(ab)^{nm} = e$. Так как k – это минимальное число со свойством $(ab)^k = e$, то $k = nm$.

(3) Все перечисленные элементы различны. Действительно, если бы было $g^i = g^j$ при $0 \leqslant i < j \leqslant$ord$(g) - 1$, то выполнялось бы $g^{j-i} = e$, что противоречит минимальности ord(g). Покажем теперь, что произвольный элемент $x \in G$ лежит в указанном множестве. Имеем $x = g^n$ для некоторого $n \in \mathbb{Z}$. Поделим n на ord(g) с остатком: $n = k\cdot$ord$(g) + r$, где $0 \leqslant r <$ord(g). Тогда $x = (g^{\mathrm{ord}(g)})^k g^r = g^r$. □

3.6. Определение подгруппы группы. *Подгруппой группы* G называется любое ее непустое подмножество H, удовлетворяющее двум условиям:

1) H замкнуто относительно умножения: для любых $h_1, h_2 \in H$ элемент h_1h_2 из группы G лежит в H.

2) H замкнуто относительно взятия обратных элементов: для любого $h \in H$ элемент h^{-1} из группы G лежит в H.

Легко проверить, что подгруппа группы G сама является группой относительно той же операции, что определена на G.

3.7. Пример. Все подгруппы группы $\mathbb{Z}_6^+$ это $\{0\}, \{0,3\}, \{0,2,4\}$ и сама группа $\mathbb{Z}_6^+$.

3.8. Упражнение. 1) Любая подгруппа циклической группы является циклической.

2) В конечной группе любое непустое подмножество, замкнутое относительно умножения, является подгруппой

Порядок группы G – это число элементов в ней, обозначается $|G|$.

3.9. Теорема Лагранжа. Порядок подгруппы конечной группы делит порядок этой группы.

Доказательство. Пусть группа G конечна и H – ее подгруппа. Если $G = H$, то доказывать нечего. Предположим, что $H = \{h_1, \dots, h_n\}$ меньше G и пусть $x \in G \setminus H$. Тогда все элементы множества $Hx = \{h_1x, \dots, h_nx\}$ различны и не совпадают с элементами из H. Действительно, из $h_ix = h_jx$ следует $h_i = h_j$, а из $h_ix = h_j$ следует $x = h_i^{-1}h_j \in H$, что невозможно. Если $H \cup Hx = G$, то теорема доказана. Если же $H \cup Hx$ меньше G, то возьмем элемент $y \in G \setminus (H \cup Hx)$ и образуем множество $Hy = \{h_1y, \dots, h_ny\}$. Аналогично доказывается, что все его элементы различны и не совпадают с элементами из $H \cup Hx$. Продолжая далее, получим разложение G в объединение n-элементных множеств $H, Hx, Hy, \dots$. Отсюда $|G|$ делится на n. □

3.10. Следствие. Порядок элемента конечной группы делит порядок этой группы.

Доказательство. Пусть G – конечная группа и g – ее элемент. Рассмотрим подгруппу $\{e, g, g^2, \dots, g^{\mathrm{ord}(g)-1}\}$ группы G, порожденную элементом g. Ее порядок ord(g) делит $|G|$ по теореме Лагранжа. □

Следующая лемма понадобится в доказательстве теоремы 4.8.

3.11. Лемма. Пусть G – конечная абелева группа и a – элемент наибольшего порядка в ней. Тогда порядок любого элемента группы G делит порядок a.

Доказательство. Пусть x – произвольный элемент из G. Если $\mathrm{ord}(x)$ не делит $\mathrm{ord}(a)$, то существует такое простое q и показатель $\alpha \geqslant 1$, что q^α делит $\mathrm{ord}(x)$ и не делит $\mathrm{ord}(a)$. Пусть $\beta \geqslant 0$ – наибольшее число такое, что q^β делит $\mathrm{ord}(a)$. Тогда $\alpha > \beta$.

Положим $y = x^{\mathrm{ord}(x)/q^\alpha}$ и $b = a^{q^\beta}$. Тогда $\mathrm{ord}(y) = q^\alpha$ и $\mathrm{ord}(b) = \mathrm{ord}(a)/q^\beta$. Так как $\mathrm{ord}(y)$ и $\mathrm{ord}(b)$ взаимно просты и группа G абелева, то $\mathrm{ord}(yb) = \mathrm{ord}(y) \cdot \mathrm{ord}(b) = \mathrm{ord}(a) q^{\alpha-\beta} > \mathrm{ord}(a)$ – противоречие. $\square$

Лекция 4
Структура мультипликативной группы кольца $\mathbb{Z}_m$

4.1. Теорема о разложении мультипликативной группы кольца $\mathbb{Z}_m$. Если $m = m_1 m_2 \dots m_s$, где m_i попарно взаимно просты, то $\mathbb{Z}_m^* \simeq \mathbb{Z}_{m_1}^* \times \dots \times \mathbb{Z}_{m_s}^*$.

Доказательство. $\mathbb{Z}_m^* \simeq (\mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s})^* = \mathbb{Z}_{m_1}^* \times \dots \times \mathbb{Z}_{m_s}^*$. $\square$

В частности, если $m = p_1^{k_1} \dots p_s^{k_s}$ – разложение на простые числа, то $\mathbb{Z}_m^* \simeq \mathbb{Z}_{p^{k_1}}^* \times \dots \times \mathbb{Z}_{p^{k_s}}^*$. Таким образом, достаточно разобраться в структуре группы $\mathbb{Z}_{p^k}^*$, где p – простое. Оказывается, что эта группа циклическая за исключением случая, когда $p = 2$, $k \geqslant 3$.

Пусть $\varphi(m)$ – *функция Эйлера*, т.е. количество чисел в ряду $1, 2, \dots, m-1$, взаимно простых с m.

4.2. Теорема о порядке мультипликативной группы кольца $\mathbb{Z}_m$.

1) Порядок группы $\mathbb{Z}_m^*$ равен $\varphi(m)$.

2) Если $m = p_1^{k_1} \dots p_s^{k_s}$ – разложение на простые числа, то $\varphi(m) = \varphi(p_1^{k_1}) \dots \varphi(p_s^{k_s})$ и $\varphi(p^k) = p^{k-1}(p-1)$ для любого простого p.

Доказательство. 1) Достаточно понять, что в группу $\mathbb{Z}_m^*$ входят все те элементы из $1, 2, \dots, m-1$, которые взаимно просты с m. По определению, a входит в $\mathbb{Z}_m^*$ тогда и только тогда, когда существует b такое, что $ab \equiv 1 \pmod m$. Ясно, что тогда a взаимно просто с m. Наоборот, если a взаимно просто с m, то по следствию 1.2 существует b такое, что $ab \equiv 1 \pmod m$ и тогда $a \in \mathbb{Z}_m^*$.

2) Так как $\mathbb{Z}_m^* \simeq \mathbb{Z}_{p^{k_1}}^* \times \dots \times \mathbb{Z}_{p^{k_s}}^*$, то в силу 1) имеем $\varphi(m) = \varphi(p_1^{k_1}) \dots \varphi(p_s^{k_s})$. Формула $\varphi(p^k) = p^k - p^{k-1}$ при p простом вытекает из того, что в ряду $1, 2, \dots, p^k - 1$ только числа кратные p не взаимно просты с p^k, а таких чисел $p^{k-1} - 1$. $\square$

4.3. Следствие (Теорема Эйлера). Если a и m взаимно просты, то

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

Доказательство. Если a и m взаимно просты, то можно считать, что $a \in \mathbb{Z}_m^*$. По следствию 3.10, порядок элемента a делит порядок группы $\mathbb{Z}_m^*$, т.е. делит $\varphi(m)$. Отсюда $a^{\varphi(m)} = 1$ в $\mathbb{Z}_m^*$. $\square$

4.4. Следствие (Малая теорема Ферма). Если p – простое и a не делится на p, то

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

Теперь перейдем к выяснению строения групп $\mathbb{Z}_{p^n}^*$ при простом p. Для доказательства следствия 4.9 необходим небольшой экскурс в теорию полей.

4.5. Определение. *Поле* – это ассоциативное, коммутативное кольцо с единицей, в котором все ненулевые элементы обратимы.

Очевидно, если K – поле, то $K^* = K \setminus \{0\}$. В частности, произведение любых ненулевых элементов поля снова ненулевой элемент.

4.6. Пример. 1) Рациональные, вещественные и комплексные числа образуют поля.
2) Кольцо вычетов $\mathbb{Z}_n$ является полем тогда и только тогда, когда n – простое.

4.7. Теорема. Любой многочлен степени n от одной переменной и с коэффициентами из поля K имеет в K не более n корней.

Доказательство этой фундаментальной теоремы содержится в любом учебнике по высшей алгебре.

4.8. Теорема. Мультипликативная группа конечного поля является циклической.

Доказательство. Пусть K – конечное поле. Докажем, что группа K^* – циклическая. Пусть $x_1, \ldots, x_n$ – все элементы группы K^* и пусть x_1 – элемент наибольшего порядка d в ней. По лемме 3.11 порядки всех элементов x_i делят d, в частности, все x_i удовлетворяют уравнению $x^d - 1 = 0$ в K. По теореме 4.7 имеем $n \leqslant d$. Однако, $d|n$ по следствию 3.10. Отсюда $n = d$ и, значит, x_1 порождает K^*. □

4.9. Следствие. Если p – простое, то $\mathbb{Z}_p^*$ – циклическая группа порядка $p-1$.

4.10. Предложение. Если $p \geqslant 3$ – простое, то группа $\mathbb{Z}_{p^n}^*$ циклическая для всех $n \geqslant 1$.

Доказательство. По следствию существует такое натуральное число g, что $g^{p-1} \equiv 1 \,(\bmod p)$ и $g^l \not\equiv 1 \,(\bmod p)$ при $1 \leqslant l < p-1$. Если $g^{p-1} \equiv 1(\bmod p^2)$, то

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + (p-1)g^{p-2}p + p^2(\ldots)\\ &\equiv 1 + (p-1)g^{p-2}p \;(\bmod p^2)\\ &\not\equiv 1 \;(\bmod p^2).\end{aligned}$$

Поэтому, беря $g+p$ вместо g, можно считать, что $g^{p-1} \not\equiv 1 \;(\bmod p^2)$. Таким образом,

$$g^{p-1} = 1 + pu$$

для некоторого u, не делящегося на p. Докажем, что вычет g порождает $\mathbb{Z}_{p^n}^*$. Сначала докажем, что при любом $k \geqslant 0$

$$g^{(p-1)p^k} = 1 + p^{k+1}u_k \tag{1}$$

для некоторого u_k, не делящегося на p. Пусть это утверждение уже доказано для некоторого $k \geqslant 0$. Докажем его для $k+1$.

$$g^{(p-1)p^{k+1}} = (1 + p^{k+1}u_k)^p = 1 + p^{k+2}u_k + \sum_{i=2}^{p} C_p^i (p^{k+1}u_k)^i.$$

Достаточно доказать, что каждое слагаемое в последней сумме делится на p^{k+3}. При $2 \leqslant i < p$ биномиальный коэффициент C_p^i делится на p и тогда слагаемое $C_p^i(p^{k+1}u_k)^i$

делится на $p^{1+i(k+1)}$. Так как $1+i(k+1) \geqslant 1+2(k+1) \geqslant k+3$, то оно делится на p^{k+3}. Слагаемое в сумме при $i=p$ делится на $p^{(k+1)p}$. Так как $(k+1)p \geqslant 3(k+1) \geqslant k+3$, то оно тоже делится на p^{k+3}. Утверждение доказано.

Перейдем к вычислению порядка вычета g в группе $\mathbb{Z}_{p^n}^*$. Этот порядок d делит порядок группы, т.е. число $\varphi(p^n) = p^{n-1}(p-1)$. Так как $g^d \equiv 1 \pmod{p^n}$, то $g^d \equiv 1 \pmod{p}$ и, значит, $(p-1)|d$. Таким образом, d имеет вид $d=(p-1)p^k$ для некоторого $k \geqslant 0$. Из утверждения (1) следует, что k не может быть меньше $n-1$. Итак, $d = \varphi(p^n)$. $\square$

Далее, если A, B – подмножества группы G, то обозначим

$$AB = \{ab \mid a \in A,\, b \in B\}.$$

Легко понять, что если группа G абелева, а A и B – ее подгруппы, то AB – тоже ее подгруппа.

4.11. Лемма. Пусть G – абелева группа и A, B – ее подгруппы такие, что $A \cap B = \{e\}$. Тогда любой элемент $g \in AB$ записывается единственным образом в виде $g = ab$, где $a \in A$ и $b \in B$. Кроме того, $AB \simeq A \times B$.

Доказательство. Предположим, что $g = ab = a_1b_1$, где $a, a_1 \in A$ и $b, b_1 \in B$. Тогда $aa_1^{-1} = bb_1^{-1}$. Поскольку $A \cap B = \{e\}$, то $a = a_1$, $b = b_1$ и единственность доказана. Изоморфизм $AB \to A \times B$ задается правилом $ab \mapsto (a, b)$. $\square$

Прежде, чем доказывать предложение 4.13, разберем следующий пример.

4.12. Пример. В группе $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$ имеются две подгруппы:

$$\begin{aligned} \langle -1\rangle &= \{(-1)^0, (-1)^1\} &&= \{1, 15\},\\ \langle 5\rangle &= \{5^0, 5^1, 5^2, 5^3\} &&= \{1, 5, 9, 13\}. \end{aligned}$$

Перемножив поэлементно эти подгруппы, получим всю группу $\mathbb{Z}_{16}^*$. Кроме того, по лемме 4.11 имеем $\mathbb{Z}_{16}^* = \langle -1\rangle\langle 5\rangle \simeq \langle -1\rangle \times \langle 5\rangle \simeq \mathbb{Z}_2^+ \times \mathbb{Z}_4^+$.

4.13. Предложение. 1) $\mathbb{Z}_2^*$ и $\mathbb{Z}_4^*$ – циклические группы порядков 1 и 2, соответственно.
2) Если $k \geqslant 3$, то $\mathbb{Z}_{2^k}^* \simeq \mathbb{Z}_2^+ \times \mathbb{Z}_{2^{k-2}}^+$ – нециклическая группа.

Доказательство. Первое утверждение проверяется непосредственно. Докажем второе. Сначала заметим, что $|\mathbb{Z}_{2^k}^*| = \varphi(2^k) = 2^{k-1}$. Далее мы докажем следующие пункты:

(а) $-1 \in \mathbb{Z}_{2^k}^*$ и -1 имеет порядок 2 в группе $\mathbb{Z}_{2^k}^*$;

(б) $5 \in \mathbb{Z}_{2^k}^*$ и 5 имеет порядок 2^{k-2} в группе $\mathbb{Z}_{2^k}^*$;

(в) $\langle -1\rangle \cap \langle 5\rangle = \{1\}$.

Тогда по лемме 4.11 произведение подгрупп $\langle -1\rangle$ и $\langle 5\rangle$ имеет порядок 2^{k-1} и, значит, совпадает с $\mathbb{Z}_{2^k}^*$. Кроме того, по лемме 4.11 это произведение изоморфно прямому произведению и предложение будет доказано.

Пункт (а) очевиден. Далее, $5 \in \mathbb{Z}_{2^k}^*$, так как 5 и 2^k взаимно просты. Докажем, что $\operatorname{ord}(5) = 2^{k-2}$. Достаточно доказать, что $5^{2^{k-2}} \equiv 1 \pmod{2^k}$ и $5^{2^l} \not\equiv 1 \pmod{2^k}$ при $l = 0, 1, \dots, k-3$, а это вытекает из следующего утверждения.

Утверждение. При любом $l \geqslant 0$ выполняется $5^{2^l} = 1 + 2^{l+2}u$ для некоторого нечетного числа u, зависящего от l.

Доказательство. При $l = 0$ утверждение очевидно. Сделаем индукционный переход от l к $l+1$:

$$5^{2^{l+1}} = (1 + 2^{l+2}u)^2 = 1 + 2^{l+3}(u + 2^{l+1}u^2).$$

Осталось заметить, что при $l \geqslant 0$ число в последних скобках нечетно.

Докажем пункт (в). Предположим, что $-1 \in \langle 5 \rangle$, т.е. $-1 \equiv 5^s \pmod{2^k}$ при некотором s. Рассматривая это сравнение по модулю 4, получаем $-1 \equiv 1 \pmod 4$ – противоречие. $\square$

4.14. Определение. Пусть q – степень простого нечетного числа. *Первообразным корнем по модулю* q называется любой порождающий мультипликативной группы $\mathbb{Z}_q^*$.

4.15. Упражнение. Пусть q – степень простого нечетного числа. Тогда

1) имеется ровно $\varphi(\varphi(q))$ первообразных корней по модулю q;

2) число a является первообразным корнем по модулю q тогда и только тогда, когда

$$a^{\frac{q-1}{p}} \not\equiv 1 \pmod q.$$

для каждого простого делителя p числа $q-1$.

Лекция 5
Квадратичный закон взаимности

5.1. Определение. Пусть p – простое число. Целое число a называется *квадратичным вычетом по модулю* p, если сравнение $x^2 \equiv a \pmod p$ имеет решение.

5.2. Предложение. Пусть p – простое нечетное число.
1) Среди чисел $\mathbb{Z}_p^* = \{1, \dots, p-1\}$ ровно половина являются квадратичными вычетами.
2) Если $a \in \mathbb{Z}_p^*$ – квадратичный вычет, то $a^{\frac{p-1}{2}} = 1$, а если нет, то $a^{\frac{p-1}{2}} = -1$.

Доказательство. 1) По следствию 4.9 в группе $\mathbb{Z}_p^*$ есть элемент z такой, что $\mathbb{Z}_p^* = \{1, z, z^2, \dots, z^{p-2}\}$. Если возвести эти элементы в квадрат, то получатся элементы $1, z^2, z^4, \dots, z^{p-3}$ и только. В самом деле, предположим, что z^k является квадратом некоторого z^l. Тогда $z^{k-2l} = 1$ и, значит, $k - 2l$ делится на $p - 1$, в частности, k – четно. Итак, только числа $1, z^2, z^4, \dots, z^{p-3}$ являются квадратичными вычетами.

2) Пусть a – квадратичный вычет, т.е. $a = x^2$ для некоторого x. Тогда $a^{\frac{p-1}{2}} = x^{p-1} = 1$. Пусть a – квадратичный невычет. Тогда $a = z^k$ для некоторого нечетного k. Имеем $a^{\frac{p-1}{2}} = z^{k\frac{p-1}{2}} \neq 1$, так как $k\frac{p-1}{2}$ не делится на $p - 1$. Однако, $\left(a^{\frac{p-1}{2}}\right)^2 = 1$. Поэтому $a^{\frac{p-1}{2}} = -1$. Здесь мы использовали то, что уравнение $x^2 = 1$ в поле $\mathbb{Z}_p$ имеет лишь 2 корня: 1 и -1.

5.3. Определение символа Лежандра $\left(\frac{a}{p}\right)$. Пусть p – простое нечетное число и a – целое число. При a, делящемся на p, полагают $\left(\frac{a}{p}\right) = 0$. При a, не делящемся на p,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ – квадратичный вычет по модулю } p, \\ -1, & \text{если } a \text{ – квадратичный невычет по модулю } p. \end{cases}$$

По предложению 5.2 имеем следующее равенство в $\mathbb{Z}_p$:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}.$$

5.4. Свойства символа Лежандра.
1) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ при b, не делящемся на p.
2) $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$.
3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Для доказательства теорем 5.6 и 5.7 нам понадобится следующая важная теорема.

5.5. Теорема о конечных полях. Для любого простого p и любого натурального $n \geqslant 1$ существует и единственно с точностью до изоморфизма поле, состоящее из p^n элементов. Это поле $GF(p^n)$ содержит в качестве подполя поле, изоморфное $\mathbb{Z}_p$. В частности, сумма p единиц в $GF(p^n)$ равна нулю. Более того, любое конечное поле изоморфно полю $GF(p^n)$ для некоторых p и n.

Доказательство этой теоремы можно найти в любом хорошем учебнике по высшей алгебре. Мы проиллюстрируем его, построив поле порядка 9. Пусть P – множество всех многочленов вида $ax+b$, где a, b пробегают поле $\mathbb{Z}_3$. Многочлены можно очевидным способом складывать и умножать. Однако, мы будем делать это по модулю многочлена x^2+1. Например, обычное произведение многочленов $x+2$ и $2x+1$ равно $2x^2+5x+2$. Нужное нам произведение равно остатку от деления $2x^2+5x+2$ на x^2+1, т.е. $5x$, что равно $2x$, так как коэффициенты рассматриваются по модулю 3. Докажем, что любой ненулевой многочлен $f(x)$ из P обратим. Если $f(x) = ax+b$, то $f(x)(ax-b) = -a^2-b^2$. Легко понять, что при $(a, b) \neq (0, 0)$ элемент $-a^2-b^2$ поля $\mathbb{Z}_3$ не равен 0 и, значит, обратим. Пусть c – обратный к нему. Тогда $(ax-b)c$ – многочлен, обратный к $f(x)$. Все остальные аксиомы поля проверяются тривиально.

5.6. Теорема. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Доказательство. Прежде всего заметим, что для любого нечетного n, число $\frac{n^2-1}{8}$ целое и по модулю 2 выполняется сравнение

$$\frac{n^2-1}{8} \equiv \begin{cases} 0, & \text{если } n = \pm 1 \pmod 8, \\ 1, & \text{если } n = \pm 5 \pmod 8). \end{cases}$$

Рассмотрим поле $GF(p^2)$. По теореме 4.8 его мультипликативная группа циклическая. Так как она имеет порядок p^2-1, то в ней существует элемент порядка 8. Обозначим его через α и положим $y = \alpha + \alpha^{-1}$. Тогда

$$y^2 = 2.$$

Действительно, $\alpha^2 + \alpha^{-2} = 0$, т.к. $\alpha^4 = -1$. Кроме того, по биному Ньютона имеем

$$y^p = \alpha^p + \alpha^{-p}.$$

Если $p = \pm 1 \pmod 8$, то отсюда выводим, что $y^p = y$. Тогда $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = y^{p-1} = 1$.

Если $p = \pm 5 \pmod 8$, то $y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y$. Тогда $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = y^{p-1} = -1$. $\square$

5.7. Теорема (Гаусс). Если p и q – простые числа, не равные 2, то

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}.$$

Доказательство. Считаем, что $p \neq q$. Рассмотрим поле $GF(p^{q-1})$. По теореме 4.8 его мультипликативная группа циклическая. Так как она имеет порядок $p^{q-1}-1$, то в ней существует элемент порядка $p^{q-1}-1$. По теореме Эйлера $p^{q-1}-1$ делится на q, и значит в этой группе имеется элемент порядка q. Обозначим его через ω. Тогда $\omega \neq 1$ и $\omega^q = 1$ в $GF(p^{q-1})$. Теперь определим *сумму Гаусса*:

$$y = \sum_{x \in \mathbb{Z}_q} \left(\frac{x}{q}\right)\omega^x.$$

Утверждение 1. Имеет место равенство

$$y^2 = (-1)^{\frac{q-1}{2}} q.$$

Доказательство.

$$y^2 = \sum_{x,z} \Big(\frac{xz}{q}\Big)\omega^{x+z} = \sum_{u\in\mathbb{Z}_q}\omega^u \sum_{x\in\mathbb{Z}_q}\Big(\frac{x(u-x)}{q}\Big).$$

Можно считать, что в последней сумме x пробегает множество $\mathbb{Z}_q \setminus \{0\}$. Далее, при $x \neq 0$,

$$\Big(\frac{x(u-x)}{q}\Big) = \Big(\frac{-x^2}{q}\Big)\Big(\frac{1-ux^{-1}}{q}\Big) = (-1)^{\frac{q-1}{2}}\Big(\frac{1-ux^{-1}}{q}\Big).$$

Отсюда

$$(-1)^{\frac{q-1}{2}} y^2 = \sum_{u\in\mathbb{Z}_q} C_u\omega^u,$$

где

$$C_u = \sum_{x\in\mathbb{Z}_q\setminus\{0\}} \Big(\frac{1-ux^{-1}}{q}\Big).$$

Очевидно

$$C_0 = \sum_{x\in\mathbb{Z}_q\setminus\{0\}} \Big(\frac{1}{q}\Big) = q-1.$$

Если $u \neq 0$, то $s = 1-ux^{-1}$ пробегает множество $\mathbb{Z}_q \setminus \{1\}$ и, поэтому,

$$C_u = \sum_{s\in\mathbb{Z}_q}\Big(\frac{s}{q}\Big) - \Big(\frac{1}{q}\Big) = -\Big(\frac{1}{q}\Big),$$

так как $\left(\frac{0}{q}\right) = 0$, а в $\mathbb{Z}_q\setminus\{0\}$ число элементов, являющихся квадратами, и число элементов, не являющихся квадратами, одинаковы. Отсюда

$$\sum_{u\in\mathbb{Z}_q} C_u\omega^u = (q-1) - \sum_{u\in\mathbb{Z}_q\setminus\{0\}} \omega^u = q,$$

что и доказывает утверждение.

Утверждение 2. Имеет место равенство

$$y^{p-1} = \Big(\frac{p}{q}\Big).$$

Доказательство. С помощью бинома Ньютона выводим

$$y^p = \sum_{x\in\mathbb{Z}_q}\Big(\frac{x}{q}\Big)\omega^{xp} = \sum_{z\in\mathbb{Z}_q}\Big(\frac{zp^{-1}}{q}\Big)\omega^z = \Big(\frac{p^{-1}}{q}\Big)y = \Big(\frac{p}{q}\Big)y,$$

откуда и следует утверждение.

Завершение доказательства теоремы. По утверждениям 1 и 2 имеем равенство

$$\Big(\frac{p}{q}\Big) = y^{p-1} = \Big((-1)^{\frac{q-1}{2}}q\Big)^{\frac{p-1}{2}} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\Big(\frac{q}{p}\Big).$$

в поле $GF(p^{q-1})$, а, значит, и в кольце натуральных чисел. □

5.8. Пример вычисления символа Лежандра.

$$\left(\frac{74}{163}\right)=\left(\frac{2}{163}\right)\left(\frac{37}{163}\right)=-\left(\frac{37}{163}\right);$$

$$\left(\frac{37}{163}\right)=\left(\frac{163}{37}\right)=\left(\frac{15}{37}\right)=\left(\frac{3}{37}\right)\left(\frac{5}{37}\right)=\left(\frac{37}{3}\right)\left(\frac{37}{5}\right)=\left(\frac{1}{3}\right)\left(\frac{2}{5}\right)=-1.$$

Поэтому

$$\left(\frac{74}{163}\right)=1.$$

Итак, 74 – квадратичный вычет по модулю 163. Однако, найти без компьютера такой x, что $74 \equiv x^2 \pmod{163}$ весьма непросто!

Опишем один из возможных способов. Для любого простого p обозначим через $\alpha(p)$ наименьший порождающий группы $\mathbb{Z}_p^*$. Из расширенной гипотезы Римана[1] следует, что $\alpha(p) \leqslant c\log^6 p$ для некоторой константы c. Таким образом, $\alpha(p)$ мало по сравнению с p. При $p < 10^4$ максимум из $\alpha(p)$ равен 31 и достигается на одном простом числе: $p = 5881$. При $p < 10^{14}$ максимум из $\alpha(p)$ равен 335. Примерно в каждом третьем случае при $p < 10^{14}$ выполняется $\alpha(p) = 2$. Проверим, что и в нашем случае это тоже так, т.е. $\alpha(163) = 2$. Итак, надо доказать, что $\mathrm{ord}(2) = 162$ в группе $\mathbb{Z}_{163}^*$. Так как $162 = 2 \cdot 3^4$, то, в силу упражнения 4.15, достаточно доказать, что $2^d \not\equiv 1 \pmod{163}$ при $d = 81$ и $d = 54$. В $\mathbb{Z}_{163}^*$ имеем,

d	1	3	9	27	81	2	6	18	54
2^d	2	8	23	105	-1	4	64	40	104

Теперь вычисляем степени 2 в группе $\mathbb{Z}_{163}^*$ до того момента, пока появится число 74:

d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2^d	2	4	8	16	32	64	128	93	23	46	92	21	42	84	5	10	20

d	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
2^d	40	80	-3	-6	-12	-24	-48	67	134	105	47	94	25	50	100	37	74

Таким образом, в группе $\mathbb{Z}_{163}^*$ справедливо $74 = 2^{34}$, значит $x = \pm 2^{17} = \pm 20$.

Заметим, что с помощью компьютера вычисление n такого, что $2^n \equiv b \pmod{p}$ очень просто: на каждом шаге надо хранить только одно число; на очередном шаге надо умножить его на 2 (дописав 0 в двоичной записи), и если результат превысит p, вычесть p. Однако, при большом p вычисление может занять много времени, поскольку надо перебирать n от 1 до $p - 1$.

---

[1]Пусть $m \in \mathbb{N}$. Числовым характером по модулю m называется любое отображение $\chi : \mathbb{Z} \to \mathbb{C}$ со свойствами

1) $\chi(a) = 0 \Leftrightarrow \textbf{нод}(a, m) > 1$,
2) $\chi(a + m) = \chi(a)$,
3) $\chi(ab) = \chi(a)\chi(b)$.

Расширенная гипотеза Римана гласит, что если χ – характер по модулю m, то нули L-функции Дирихле

$$L(\chi, s) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s}$$

в полосе $0 < \mathrm{Re}\, s < 1$ лежат на прямой $\mathrm{Re}\, s = 1/2$.

Более быстрый способ основан на следующем соображении. Пусть p – нечетное простое число и a – квадратичный вычет по модулю p. Тогда $a^{\frac{p-1}{2}} \equiv 1 \,(\mathrm{mod}\, p)$ и $a^{\frac{p+1}{2}} \equiv a \,(\mathrm{mod}\, p)$. Если число $\frac{p+1}{2}$ четно, то сравнение $x^2 \equiv a \,(\mathrm{mod}\, p)$ решается легко: $x \equiv \pm a^{\frac{p+1}{4}} \,(\mathrm{mod}\, p)$. В нашем случае $x \equiv \pm 74^{41} \,(\mathrm{mod}\, 163)$. Последний вычет ищется быстро с помощью последовательного возведения вычетов в квадрат (учесть, что $41 = 2^5 + 2^3 + 2^0$):

d	0	1	2	3	4	5
74^{2^d}	74	97	118	69	34	15

Отсюда $x \equiv \pm(74 \cdot 69 \cdot 15) \,(\mathrm{mod}\, 163) \equiv \pm 20 \,(\mathrm{mod}\, 163)$.

5.9. Решение сравнения $x^2 \equiv a \,(\mathrm{mod}\, p)$, где p – нечетное простое число. Из п. 5.2 следует, что это сравнение разрешимо тогда и только тогда, когда a – квадратичный вычет по модулю p, т.е.

$$a^{\frac{p-1}{2}} \equiv 1 \,(\mathrm{mod}\, p).$$

Предположим, что последнее выполняется. Предположим также, что мы знаем некоторый квадратичный невычет N по модулю p, т.е. мы знаем N со свойством

$$N^{\frac{p-1}{2}} \equiv -1 \,(\mathrm{mod}\, p).$$

Пусть $p - 1 = 2^s l$, где l нечетно. Будем последовательно находить числа $b_{s-1}, \dots, b_0$ такие, что

$$(a^l b_i^2)^{2^i} \equiv 1 \,(\mathrm{mod}\, p).$$

Можно положить $b_{s-1} = 1$. Если b_i уже найдено и $i > 0$, то, извлекая корень, получим, что $(a^l b_i^2)^{2^{i-1}}$ сравнимо с 1 или -1 по модулю p. В первом случае положим $b_{i-1} = b_i$, во втором $b_{i-1} = b_i N^{\frac{p-1}{2^{i+1}}}$. В конце получим $a^l b_0^2 \equiv 1 \,(\mathrm{mod}\, p)$, откуда $(a^{\frac{l+1}{2}} b_0)^2 \equiv a \,(\mathrm{mod}\, p)$ и, значит,

$$x \equiv \pm a^{\frac{l+1}{2}} b_0 \,(\mathrm{mod}\, p).$$

5.10. Замечание. Мы знаем, что половина чисел из множества $\{1, 2, \dots, p-1\}$ являются квадратичными вычетами по модулю p, а половина – нет. Поэтому с помощью случайного выбора числа в этом множестве можно с вероятностью $1/2$ найти квадратичный невычет. В 1952 году Анкени доказал, что при условии выполнения расширенной гипотезы Римана существует такое $C > 0$, что наименьший квадратичный невычет по модулю p не превосходит $C \log^2 p$. Для некоторых $p \equiv 1 \,(\mathrm{mod}\, 4)$ квадратичный невычет N известен заранее; например, $N = 2$ при $p \equiv 5 \,(\mathrm{mod}\, 8)$.

Поиск решений уравнения $x^2 \equiv a \,(\mathrm{mod}\, n)$, в случае, когда n – составное и нам неизвестно разложение n на простые числа, является трудной задачей.

5.11. Упражнение. 1) Написать программу, находящую наименьший квадратичный невычет $N(p)$ по модулю заданного простого числа p.

2) Найти максимум из $N(p)$ при $2 < p < 10^6$. На каких p достигается этот максимум?

3) Построить график функции $p \mapsto \frac{N(p)}{\log^2 p}$ и найти ее максимум при $10^5 < p < 10^6$.

Лекция 6
Задача дискретного логарифмирования

6.1 Формулировка задачи. Пусть p – нечетное простое число, a – порождающий группы $\mathbb{Z}_p^*$ (таким образом, $\mathrm{ord}(a) = p-1$), и b – число, не делящиеся на p. Найти n такое, что

$$a^n \equiv b \,(\bmod p). \tag{2}$$

Пишут $n = \log_a b$. В следующем пункте описывается алгоритм, работающий очень быстро в случае, когда число p *гладкое*, т.е. когда $p-1$ разлагается в произведение малых[2] простых чисел, и это разложение известно.

6.2. Алгоритм LOGsmooth. Пусть q – простое число, делящее $p-1$. Тогда множество решений уравнения $x^q = 1$ в поле $\mathbb{Z}_p$ состоит из элементов $1, c, c^2, \ldots, c^{q-1}$, где $c \equiv a^{\frac{p-1}{q}} \,(\bmod p)$. Если дано число d и известно, что оно удовлетворяет уравнению $x^q = 1$, то можно перебором найти t такое, что $d = c^t$ и $0 \leqslant t \leqslant q-1$. Здесь мы пользуемся предположением о малости q.

Далее, допустим $p-1 = q^k l$, где q и l взаимно просты. Мы будем последовательно находить (это описывается далее) числа u_i, $i = 0, 1, \ldots, k$, для которых выполняется

$$(ba^{-u_i})^{lq^{k-i}} \equiv 1 \,(\bmod p). \tag{3}$$

При $i = k$ это даст нам сравнение

$$(ba^{-u_k})^l \equiv 1 \,(\bmod p),$$

что в силу (2) эквивалентно

$$a^{(n-u_k)l} \equiv 1 \,(\bmod p).$$

Так как $\mathrm{ord}(a) = p-1$, то последнее означает, что $(n-u_k)l$ делится на $p-1$, т.е.

$$n \equiv u_k \,(\bmod q^k).$$

Выписав такие сравнения для каждого простого делителя q числа $p-1$, можно с помощью китайской теоремы об остатках найти $n \,(\bmod p-1)$.

Осталось объяснить, как искать числа u_i, удовлетворяющие сравнениям (3). Можно положить $u_0 = 1$. Если некоторое u_i уже найдено, то из (3) следует, что $(ba^{-u_i})^{lq^{k-i-1}}$ удовлетворяет уравнению $x^q \equiv 1 \,(\bmod p)$. Тогда можно найти t такое, что

$$(ba^{-u_i})^{lq^{k-i-1}} \equiv c^t \,(\bmod p).$$

Положим $u_{i+1} = u_i + tq^i$. Тогда

$$(ba^{-u_{i+1}})^{lq^{k-i-1}} \equiv c^t a^{-tlq^{k-1}} \equiv 1 \,(\bmod p),$$

что и означает выполнение (3) при $i+1$. □

[2]Понятие гладкости неформально и малость чисел не уточняется. Во всяком случае, для современных компьютеров малыми можно считать числа до 10^{10}.

Таким образом, поиск u_k осуществляется по схеме: $u_0 = 1$, $r_i \equiv (ba^{-u_i})^{lq^{k-i-1}} \pmod p$, $t_i = \log_c r_i$, $u_{i+1} = u_i + t_i q^i$.

6.3. Пример. Найдем n такое, что $2^n \equiv 74 \pmod{163}$.

Здесь $a = 2$, $b = 74$, $p = 163$ и $p - 1 = 2 \cdot 3^4$.

Положим сначала $q = 3$. Тогда $k = 4$ и $l = 2$. Кроме того, $c \equiv 2^{\frac{p-1}{3}} = 2^{54} \equiv 104 \pmod{163}$, $c^2 \equiv 58 \pmod{163}$. Теперь можно заполнить следующую таблицу:

i	0	1	2	3
r_i	1	58	1	104
t_i	0	2	0	1
u_{i+1}	1	7	7	34

Отсюда имеем $n \equiv 34 \pmod{81}$. (4)

Теперь положим $q = 2$. Тогда $k = 1$ и $l = 81$. Кроме того, $c \equiv 2^{\frac{p-1}{2}} \equiv -1 \pmod{163}$. Заполняем таблицу:

i	0
r_i	-1
t_i	1
u_{i+1}	2

Отсюда имеем $n \equiv 2 \pmod 2$. (5)

Из (4) и (5) выводим, что $n \equiv 34 \pmod{162}$.

6.4. Задачи для программирования.

1. Написать программу на C^{++}, ввод которой – простое число p, вывод – число $\alpha(p)$, являющееся наименьшим порождающим группы $\mathbb{Z}_p^*$.

Указание. а) Как уже было отмечено, $\alpha(p)$ мало по сравнению с p, поэтому $\alpha(p)$ можно находить перебором.

б) Пусть $1 < n < p - 1$. Чтобы проверить, является ли n порождающим группы $\mathbb{Z}_p^*$, надо последовательно считать степени n по модулю p. Если $n^k \equiv 1 \pmod p$ при некотором $1 < k < p - 1$, то n – не порождающий. Если же $n^k \not\equiv 1 \pmod p$ при всех $1 < k < p - 1$, то n – порождающий. Можно немного сэкономить, считая, что $k \leqslant \frac{p-1}{2}$.

Если простые множители числа $p-1$ известны, то можно воспользоваться упражнением 4.14.2).

2. Найти $\alpha_0 = \max\{\alpha(p) : p < 10^6\}$. Перечислить все $p < 10^6$, на которых этот максимум достигается.

3. Для каждого $n \in \{2, 3, \ldots, \alpha_0\}$ найти число простых чисел $p < 10^6$, для которых $\alpha(p) = n$.

4. Написать программу, реализующую алгоритм LOGsmooth из пункта 6.1.

5. Найти n такое, что $23^n \equiv 1000 \pmod{2161}$.

6. Существует ли простое p, для которого $\alpha(p) = 108$? Ответ на этот вопрос неизвестен (2005 год). Известно лишь, что p не может быть меньше 10^{14}.

6.5. Задача теоретическая. Доказать, что для всякого n существует простое число p такое, что $\alpha(p) > n$.

Решение. Пусть $q_1, \ldots, q_s$ – все простые числа, не превосходящие n, и пусть q – их произведение. По теореме Дирихле[3] в арифметической последовательности $(1+8qt)_{t\in\mathbb{N}}$ существует простое число p. Тогда $\left(\frac{q_i}{p}\right) = 1$ для любого q_i. Для $q_i = 2$ это вытекает из теоремы 5.6, а для нечетных q_i – из теоремы 5.7 и свойства 5.4.2): $\left(\frac{q_i}{p}\right) = \left(\frac{p}{q_i}\right) = \left(\frac{1+q_i(8qt/q_i)}{q_i}\right) = \left(\frac{1}{q_i}\right) = 1$. Из свойства 5.4.3) следует, что $\left(\frac{m}{p}\right) = 1$ для любого $m \leqslant n$. В силу $\left(\frac{m}{p}\right) = m^{\frac{p-1}{2}}$ это означает, что порядок числа m в группе $\mathbb{Z}_p^*$ не превосходит $\frac{p-1}{2}$. Поэтому любое $m \leqslant n$ не может быть порождающим группы $\mathbb{Z}_p^*$ и, значит, $\alpha(p) > n$. □

6.5. Историческая справка. В 1927 году Артин сформулировал гипотезу, известную теперь как *гипотеза Артина* о том, что для любого целого a, отличного от ± 1 и полного квадрата, существует бесконечно много простых чисел p, для которых a является первообразным корнем. Более того, для $N_a(x)$ – количества таких простых чисел, не превосходящих x, он привел асимптотическую формулу вида

$$N_a(x) \sim \frac{C_a x}{\ln x} \quad (x \to +\infty),$$

где $C_a > 0$ – некоторая константа. В 1967 году Хооли доказал обе эти гипотезы при условии справедливости расширенной гипотезы Римана. При этом получилось, что

$$C_2 = \prod_{q-\text{простое}} \left(1 - \frac{1}{q(q-1)}\right) = 0,3739\ldots.$$

Если же не использовать расширенную гипотезу Римана, то неизвестно, является ли 2 первообразным корнем для бесконечного множества простых чисел. В 1984 году Гупта и Марти доказали, что для любых трех различных простых чисел q, r и s в множестве

$$\{qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3, qrs\}$$

найдется по крайней мере одно число, являющееся первообразным корнем для бесконечного множества простых чисел. Анализируя их доказательство, Хеф-Браун доказал в 1986 году, что

(1) число простых чисел a, для которых гипотеза Артина неверна, не превосходит 2;

(2) число целых чисел, меньших x, для которых гипотеза Артина неверна, не превосходит $\log^2 x$ при всех достаточно больших x.

6.6. Упражнение. Доказать, что в предположениях п. 6.1 о числах p, a и b решение уравнения $a^n \equiv b \pmod{p}$ можно находить по формуле

$$n \equiv \sum_{i=1}^{p-2} (1-a^i)^{-1} b^i \pmod{p-1},$$

где обратный берется в группе $\mathbb{Z}_p^*$.

[3]**Теорема Дирихле (1839).** Пусть a и d – взаимно простые натуральные числа. Тогда в арифметической последовательности $a, a+d, a+2d, \ldots$ существует простое число.

Лекция 7
Вероятностные тесты на простоту

7.1. Псевдопростые числа. Малая теорема Ферма утверждает, что если n – простое и a взаимно просто с n, то
$$a^{n-1} \equiv 1 \pmod{n}. \tag{6}$$

Однако и для составных чисел n и некоторых взаимно простых с ними чисел a это сравнение может выполняться. Например,
$$7^{24} \equiv 1 \pmod{25}.$$

7.1.1. Определение. Число n называется *псевдопростым по основанию* a, если n составное и выполняется сравнение (6).

Таким образом, 25 является псевдопростым по основанию 7. Однако, 25 не является псевдопростым по основаниям $2, 3, 4, 5$ и 6:
$$2^{24} \equiv 16 \pmod{25}, \quad 3^{24} \equiv 14 \pmod{25}, \quad 4^{24} \equiv 6 \pmod{25},$$
$$5^{24} \equiv 0 \pmod{25}, \quad 6^{24} \equiv -1 \pmod{25}.$$

Следующее предложение и упражнение отвечают на вопрос:
Для скольки a из $\mathbb{Z}_n^*$ число n является псевдопростым по основанию a?
Положим
$$B_n = \{a \in \mathbb{Z}_n^* \mid a^{n-1} = 1\}.$$

7.1.2. Предложение. Если n простое, то $B_n = \mathbb{Z}_n^*$. Если n – составное, то
$$B_n = \mathbb{Z}_n^* \quad \text{или} \quad |B_n| \leqslant \frac{1}{2}|\mathbb{Z}_n^*|.$$

Доказательство. Первое утверждение вытекает из малой теоремы Ферма. Для доказательства второго достаточно заметить, что B_n является подгруппой группы $\mathbb{Z}_n^*$ и что порядок подгруппы делит порядок группы. □

7.1.3. Упражнение. Пусть n – нечетное число и $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, где $p_1, p_2, \dots, p_r$ – различные простые числа. Тогда
$$|B_n| = \prod_{i=1}^{r} \textbf{нод}\,(n-1, p_i - 1).$$

Указание. Решение можно вывести из доказательства теоремы 7.2.1 и леммы 7.5.1.

Например, $91 = 7 \cdot 13$ является псевдопростым для 36 чисел из $\mathbb{Z}_{91}^*$ и не является псевдопростым для остальных 36 чисел из $\mathbb{Z}_{91}^*$. Оказывается, существуют числа n, псевдопростые по всем основаниям $a \in \mathbb{Z}_n^*$. Такие числа называются числами Кармайкла. Наименьшее из них $561 = 3 \cdot 11 \cdot 17$.

7.2. Числа Кармайкла. Число n называется *числом Кармайкла*, если оно составное и для любого $a \in \mathbb{Z}_n^*$ выполняется $a^{n-1} = 1$ в $\mathbb{Z}_n^*$.

7.2.1. Теорема (Кармайкл, 1912). (1) Нечетное число n является числом Кармайкла тогда и только тогда, когда $n = p_1 p_2 \ldots p_r$, где p_i – различные простые числа и $n-1$ делится на $p_i - 1$ при всех i.

(2) Число Кармайкла разлагается в произведение не менее 3 различных простых чисел.

Доказательство. (1) Пусть $n = p_1^{e_1} \ldots p_r^{e_r}$ – разложение n на простые числа. По теореме 4.1 имеем изоморфизм групп

$$\mathbb{Z}_n^* \to \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^*.$$

Поэтому, если для любого $a \in \mathbb{Z}_n^*$ выполняется $a^{n-1} = 1$, то и для любого $a_i \in \mathbb{Z}_{p_i^{e_i}}^*$ выполняется $a_i^{n-1} = 1$. По предложению 4.10 группа $\mathbb{Z}_{p_i^{e_i}}^*$ циклическая, т.е. в ней имеется элемент a_i порядка $|\mathbb{Z}_{p_i^{e_i}}^*| = \phi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$. Поэтому $n-1$ делится на этот порядок, а значит $e_i = 1$ и $n-1$ делится на $p_i - 1$.

Наоборот, если $e_i = 1$ и $n-1$ делится на $p_i - 1$ при всех i, то для любого $a_i \in \mathbb{Z}_p^*$ выполняется $a_i^{n-1} = 1$. Значит, для любого $a \in \mathbb{Z}_n^*$ выполняется $a^{n-1} = 1$.

(2) Предположим, что n – число Кармайкла и $n = pq$, где p, q – различные простые числа. Тогда $n-1$ делится на $p-1$ и $q-1$. Имеем $n-1 = (p-1)q + (q-1)$. Тогда $p-1$ делится на $q-1$. Аналогично $q-1$ делится на $p-1$, откуда $p = q$ – противоречие. □

7.2.2. Упражнение. 1) Проверить, что 561 – наименьшее число Кармайкла.

2) Проверить, что 101101 – число Кармайкла.

3) Доказать, что если для некоторого натурального k числа $6k+1, 12k+1, 18k+1$ – простые, то их произведение – число Кармайкла. Найти число Кармайкла, большее 10^9.

4) Проверить, что имеется ровно 16 чисел Кармайкла, меньших 10^5, и это числа $561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361$. Для всех этих чисел n найти отношение $\phi(n)/n$.

Пусть $C(n)$ – количество чисел Кармайкла меньших n. В 1994 году Альфорд, Гранвилль и Померанс доказали, что $C(n) > n^{2/7}$, начиная с некоторого n. В частности, чисел Кармайкла имеется бесконечно много. Известно также, что $\lim\limits_{n\to+\infty} \frac{C(n)}{n} = 0$. Некоторые значения $C(10^n)$ приведены в следующей таблице:

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$C(10^n)$	1	7	16	43	105	255	646	1547	3605	8241	19279	44706	105212	246683	585355

7.3. Общая структура вероятностных тестов на простоту. Пусть далее n нечетно. Несколько вероятностных тестов на простоту, включая тест Миллера – Рабина, имеют следующую общую структуру. Предположим, что для каждого нечетного n определено подмножество $L_n \subseteq \mathbb{Z}_n^*$ и число $0 < c < 1$ такие, что выполнены следующие условия:

- существует эффективный алгоритм, определяющий по $a \in \mathbb{Z}_n$, лежит ли a в L_n;
- если n – простое, то $L_n = \mathbb{Z}_n^*$;
- если n – составное, то $|L_n| \leqslant c\,\phi(n)$, где ϕ – функция Эйлера.

Выбираем некоторое натуральное число s (от него зависит погрешность теста).

Тест. Выбираем случайно s чисел $a_1, \ldots, a_s$ в множестве $\{1, \ldots, n-1\}$. Проверяем, лежат ли a_i в L_n. Если некоторое a_i не лежит в L_n, то выдается ответ: n – составное. Если все a_i лежат в L_n, то выдается ответ: n – простое с вероятностью $\geqslant 1 - c^s$.

Пояснение. Если тест выдал ответ: n – составное, то n действительно составное. В самом деле, этот ответ выдается только в том случае, когда некоторое a_i лежит вне L_n. Но для простых n это невозможно, поскольку для них $a_i \in \{1, \ldots, n-1\} = \mathbb{Z}_n^* = L_n$.

Если же тест выдал ответ: n – простое с вероятностью $\geqslant 1 - c^s$, то на основании этого мы не можем утверждать, что n простое. Можно лишь согласиться с предложенной вероятностью (и далее проверять простоту n другими средствами). В самом деле, если n составное, то событие "все a_i лежат в L_n" происходит с вероятностью $\leqslant c^s$.

Замечание. 1) Обычно тест проводится в s шагов, на каждом шаге выбирается случайно одно число в множестве $\{1, \ldots, n-1\}$. При этом выборы должны быть независимыми. Обеспечить эту независимость заранее заданной процедурой сложно.

2) При $c = 1/4$ и $s = 10$ имеем $1 - c^s > 0,99999904$. Далее будет обсуждаться, как повысить надежность этого теста.

Можем ли мы положить

$$L_n = \{a \in \mathbb{Z}_n^* \,|\, a^{n-1} = 1\}?$$

Если заранее известно, что испытуемое n не является числом Кармайкла, то в силу предложения 7.1.2 выполняется $|L_n| \leqslant \phi(n)/2$ и можно применить тест с константой $c = 1/2$. Если же n – число Кармайкла, то $L_n = \mathbb{Z}_n^*$ и, значит, $|L_n| = \phi(n)$. Поэтому L_n не удовлетворяет условиям, сформулированным перед тестом. Опыт показывает, что этот тест для произвольного числа Кармайкла выдает дезинформирующий ответ, что оно простое с большой вероятностью. Слабым утешением служит то, что числа Кармайкла встречаются редко.

Упражнение. Напишите программу для теста на простоту с $L_n = \{a \in \mathbb{Z}_n^* \,|\, a^{n-1} = 1\}$ и $c = 1/2$. Для числа Кармайкла $n = 561$ повторите тест с параметром $s = 2$ независимо сто раз. Сколько раз тест выдаст ответ: "561 — простое с вероятностью $\geqslant 3/4$"?

Следующее усиление малой теоремы Ферма позволяет определить L_n, удовлетворяющее условиям, сформулированным перед тестом при $c = 1/4$ для любого $n \neq 9$.

7.4 Усиление малой теоремы Ферма. Пусть n – простое число и $n - 1 = m2^h$, где m – нечетно. Тогда при a взаимно простом с n выполняется

$$a^m \equiv 1 \pmod{n} \quad \text{или} \quad \exists\, t,\, 0 \leqslant t < h: \;\; a^{m2^t} \equiv -1 \pmod{n}.$$

Доказательство. Согласно малой теореме Ферма, $a^n - 1$ делится на n. Далее,

$$a^n - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \ldots (a^{2^h m} + 1).$$

Так как n простое, то один из множителей делится на n.□

7.5. Тест Миллера – Рабина. Это тест из пункта 7.3 с L_n, определенным следующим образом. Предположим, что n нечетно и пусть $n - 1 = m2^h$, где m нечетно, $h \geqslant 1$. Положим

$$L_n = \{a \in \mathbb{Z}_n \,|\, a^m \equiv 1 \pmod{n} \;\; \text{или} \;\; \exists\, i,\, 0 \leqslant i < h: \;\; a^{m2^i} \equiv -1 \pmod{n)}\}.$$

Докажем, что L_n, где $n \neq 9$, удовлетворяет условиям из пункта 7.3 при $c = 1/4$. Нам понадобится следующая лемма.

7.5.1. Лемма. Пусть G – циклическая группа порядка n по умножению. Число решений уравнения $x^m = 1$ в G равно $\textbf{нод}\,(n, m)$. Более того, если для $g \in G$ уравнение $x^m = g$ разрешимо, то число его решений равно $\textbf{нод}\,(n, m)$.

Доказательство. Пусть G порождается элементом a, в частности $\mathrm{ord}(a) = n$. Элемент a^d является решением уравнения $x^m = 1$ тогда и только тогда, когда dm делится на n, т.е. когда d делится на $\frac{n}{\textbf{нод}\,(n,m)}$. По модулю n таких чисел d ровно $\textbf{нод}\,(n, m)$ штук.

Обозначим через A множество решений уравнения $x^m = 1$. Если уравнение $x^m = g$ имеет некоторое решение x_0, то $x_0 A$ – множество всех его решений. □

7.5.2. Теорема (Монье-Рабин). Пусть n – нечетное число. Если n – простое, то $L_n = \mathbb{Z}_n^*$. Если n – составное и отлично от 9, то $|L_n| \leqslant \phi(n)/4$.

Доказательство. Пусть $n - 1 = m2^h$, где m нечетно, $h \geqslant 1$. Разберем три случая.
Случай 1: n – простое. Тогда утверждение вытекает из п. 7.4.

Случай 2: $n = p^e$, где p – простое и $e > 1$. Очевидно $L_n \subseteq \{a \in \mathbb{Z}_n^* \mid a^{m2^h} = 1\}$. По лемме 7.5.1 мощность последнего множества равна

$$\textbf{нод}(|\mathbb{Z}_n^*|, n-1) = \textbf{нод}\big(p^{e-1}(p-1), p^e - 1\big) = p - 1 = \frac{\phi(n)}{p^{e-1}} < \frac{\phi(n)}{4}.$$

Случай 3: $n = p_1^{e_1} \dots p_r^{e_r}$ – разложение n на простые числа, $r > 1$. По теореме 4.1 существует изоморфизм групп

$$\theta : \mathbb{Z}_n^* \to \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^*.$$

Обозначим $\theta(a) = (a_1, \dots, a_r)$, $G = \mathbb{Z}_n^*$ и $G_i = \mathbb{Z}_{p_i^{e_i}}^*$.

Пусть $\phi(p_i^{e_i}) = m_i 2^{h_i}$, где m_i нечетно. По предложению 4.10, G_i – циклическая группа порядка $m_i 2^{h_i}$. Положим $l = \min\{h, h_1, \dots, h_r\}$. Тогда $l \geqslant 1$, поскольку n нечетно.

Утверждение. Для любого $a \in L_n$ выполняется $a^{m2^l} = 1$ в $\mathbb{Z}_n$.

Доказательство. Предположим, что $a^{m2^l} \neq 1$ для некоторого $a \in L_n$. Из определения L_n следует, что $a^{m2^h} = 1$, поэтому $l < h$ и существует такое j, что

$$a^{m2^l} \neq 1, \dots, a^{m2^j} \neq 1,\ a^{m2^{j+1}} = 1, \dots, a^{m2^h} = 1.$$

Тогда из определения L_n следует, что $a^{m2^j} = -1$, а значит, $a_i^{m2^j} = -1$ для любого $i = 1, \dots, r$. Отсюда $\mathrm{ord}(a_i^m) = 2^{j+1}$ в группе G_i. Так как порядок элемента делит порядок группы, то $j + 1 \leqslant h_i$. Имеем $l < j + 1 \leqslant h_i$ для любого i. Вспоминая, что $l < h$, получаем противоречие. □

Из определения L_n из этого утверждения вытекает, что для любого $a \in L_n$ выполняется $a^{m2^{l-1}} = \pm 1$. По лемме 7.5.1 имеем

$$\begin{aligned} |L_n| &\leqslant |\{a \in G \mid a^{m2^{l-1}} = \pm 1\}| \\ &\leqslant 2|\{a \in G \mid a^{m2^{l-1}} = 1\}|. \end{aligned}$$

Обозначим $A = \{a \in G \mid a^{m2^{l-1}} = 1\}$, $A_i = \{a_i \in G_i \mid a_i^{m2^{l-1}} = 1\}$, $i = 1, \dots, r$. Тогда $\theta(A) = A_1 \times \cdots \times A_r$. По лемме 7.5.1 имеем

$$|A_i| = \textbf{нод}\,(|G_i|, m2^{l-1}) = \textbf{нод}\,(m_i 2^{h_i}, m2^{l-1}) \leqslant \frac{1}{2}|G_i|,$$

поскольку $h_i \geqslant l$. Отсюда

$$|L_n| \leqslant 2\prod_{i=1}^{r}|A_i| \leqslant 2\prod_{i=1}^{r}\frac{1}{2}|G_i| = 2^{1-r}|G| = 2^{1-r}\phi(n).$$

Если $r \geqslant 3$, то $|L_n| \leqslant \frac{1}{4}|G|$. При $r = 2$ необходимо более точно оценить $|A_i|$. Если для некоторого $i = 1, 2$ выполняется условие

$$\textbf{нод}\,(m_i, m) < m_i \quad \text{или} \quad h_i > l, \tag{7}$$

то $|A_i| \leqslant \frac{1}{4}|G_i|$ и снова $|L_n| \leqslant \frac{1}{4}|G|$.

Пусть теперь $r = 2$ и для всех i условие (7) не выполняется. Тогда m делится на m_i и $h_i = l$ для всех i. Так как $h \geqslant l$, то $m2^h$ делится на $m_i 2^{h_i}$ для всех i. Тогда для любого $a_i \in G_i$ имеем $a_i^{n-1} = a_i^{m2^h} = 1$ и, значит, для любого $a \in G$ выполняется $a^{n-1} = 1$. Таким образом, n – число Кармайкла. Так как для чисел Кармайкла всегда $r \geqslant 3$, то получаем противоречие. $\square$

7.6. Сильно псевдопростые числа и достоверные тесты на простоту. Напомним усиление малой теоремы Ферма. Пусть n – простое число и $n - 1 = m2^h$, где m – нечетно. Тогда при a взаимно простом с n выполняется

$$a^m \equiv 1\,(\bmod\, n) \quad \text{или} \quad \exists\, t,\, 0 \leqslant t < h:\;\; a^{m2^t} \equiv -1\,(\bmod\, n). \tag{8}$$

Однако, и для составных n и некоторых взаимно простых с ними a условие (8) может выполняться. Оно выполняется, например, для чисел $n = 781 = 11 \cdot 71$ и $a = 5$.

7.6.1. Определение. Пусть n – нечетное число и $n - 1 = m2^h$, где m – нечетно. Тогда число n называется *сильно псевдопростым по основанию* a, если оно составное и выполняется условие (8).

Очевидно, если n сильно псевдопросто по основанию a, то n псевдопросто по основанию a. Числа Кармайкла n псевдопросты по всем основаниям $a \in \mathbb{Z}_n^*$. Замечательно, что по теореме Рабина для любого составного числа $n \neq 9$ (в том числе для любого числа Кармайкла) количество тех $a \in \mathbb{Z}_n^*$, для которых n сильно псевдопросто по основанию a, не превосходит $|\mathbb{Z}_n^*|/4$.

Для составного n обозначим через $a(n)$ минимальное a такое, что n не сильно псевдопросто по основанию a. Если бы удалось оценить $a(n)$ сверху некоторой “малой функцией” $f(n)$, то проверка на простоту была бы быстрой и достоверной: достаточно было бы проверить условие (8) для всех $a \leqslant f(n)$. Если условие (8) выполнено для всех $a \leqslant f(n)$, то n – простое. Если условие (8) не выполнено для некоторого $a \leqslant f(n)$, то n – составное.

Следующая теорема показывает, что при условии справедливости расширенной гипотезы Римана можно взять $f(n) = 2\log^2 n$. Это подтверждают и экспериментальные данные.

7.6.2. Теорема (Миллер). Если верна расширенная гипотеза Римана и n является сильно псевдопростым по всем основаниям из интервала от 1 до $2\log^2 n$, то n – простое.

Замечание. Альфорд, Гранвилль и Померанс доказали, что существует бесконечно много нечетных составных n, являющихся сильно псевдопростыми по всем основаниям из интервала от 1 до $(\log n)^{\frac{1}{3\log\log\log n}}$.

Следующая теорема полезна при достоверной проверке на простоту чисел до $3 \cdot 10^{15}$.

7.6.3. Теорема (Померанс, Сэлфридж, Вагстафф и Ешке).

1) Если $n < 2\,047$ сильно псевдопростое по основанию 2, то n – простое.

2) Если $n < 1\,373\,653$ сильно псевдопростое по основаниям 2 и 3, то n – простое.

3) Если $n < 25\,326\,001$ сильно псевдопростое по основаниям $2, 3$ и 5, то n – простое.

4) Если $n < 118\,670\,087\,467$ сильно псевдопростое по основаниям $2, 3, 5$ и 7, то либо $n = 3\,215\,031\,751$, либо n – простое.

5) Если $n < 2\,152\,302\,898\,747$ сильно псевдопростое по основаниям $2, 3, 5, 7$ и 11, то n – простое.

6) Если $n < 3\,474\,749\,660\,383$ сильно псевдопростое по основаниям $2, 3, 5, 7, 11$ и 13, то n – простое.

7) Если $n < 341\,550\,071\,728\,321$ сильно псевдопростое по основаниям $2, 3, 5, 7, 11, 13$ и 17, то n – простое.

8) Если $n < 4\,759\,123\,141$ сильно псевдопростое по основаниям $2, 7$ и 61, то n – простое.

9) Если $n < 10^{12}$ сильно псевдопростое по основаниям $2, 13, 23$ и 1662803, то n – простое.

7.6.4. Упражнение. 1) Покажите, что число Кармайкла 561 не является сильно псевдопростым по основанию 2.

2) Найдите наименьшее a такое, что число Кармайкла 101101 не является сильно псевдопростым по основанию a.

3) Проверьте, что $3\,215\,031751 = 151 \cdot 751 \cdot 28351$ – сильно псевдопростое по основаниям 2,3,5 и 7.

4) Напишите программу, проверяющую простоту чисел, меньших $341\,550\,071\,728\,321$, с помощью результатов пункта 7.6.3.

5) Какова вероятность ответа “n – простое ...” в тесте Миллера – Рабина для числа $n = 2047 = 23 \cdot 89$ при $s = 2$? Повторите тест Миллера – Рабина для числа 2047 с параметром $s = 2$ независимо двести раз. Сколько раз тест выдаст ответ: “простое с вероятностью $\geqslant 1 - (1/4)^2$”?

6) Примените тест Миллера-Рабина к числу 1111111111111111111. В лекции 9 появится метод, позволяющий доказать, что это число простое.

7) Примените тест Миллера-Рабина к числу

$$\lfloor \pi 10^{37} \rfloor = 31415926535897932384626433832795028841.$$

Доказано, что это число простое.

8) Проверьте, что следующее число Арнолта составное[4] и является сильно псевдопростым по всем простым основаниям, меньшим 200:

A=8038374574536394912570796143419421081388376882875581458374889175222974273765333652186502336163960045457915042023603208766569966760987284043965408232928738791850869166857328267761771029389697739470167082304286871099974399765441448453411558724506334092790222752962294149842306881685404326457534018329786111298960644845216191652872597534901.

9) Проверьте, что наименьшее простое число, превосходящее число Арнолта A, есть $A + 1900$.

[4]Ввод этого числа в мой компьютер занял 10 минут, проверка того, что оно составное произошла мгновенно. Замечу, что это 337-значное число разлагается на два простых множителя, наибольший из которых имеет 169 знаков. Сможете ли Вы по этой информации найти эти множители?

Лекция 8
Оценка функции Чебышева

Целью этой лекции является следствие 8.4; оно используется в следующей лекции.

Функция Чебышева θ определяется для любого вещественного $x > 0$ формулой

$$\theta(x) = \sum_{p \leqslant x} \ln p,$$

где суммирование ведется по всем простым числам $p \leqslant x$.

8.1. Лемма. При $n \geqslant 1$ справедливы неравенства

$$4^n > C_{2n}^n \geqslant \frac{4^n}{2\sqrt{n}}.$$

Доказательство. Неравенство $4^n > C_{2n}^n$ вытекает из формулы

$$2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} C_{2n}^i.$$

Второе неравенство докажем индукцией по n. При $n = 1$ оно справедливо. Предположим, оно справедливо при $n = k$ и докажем его при $n = k + 1$:

$$C_{2(k+1)}^{k+1} = \frac{2(2k+1)}{k+1} C_{2k}^k \geqslant \frac{2(2k+1)}{k+1} \frac{4^k}{2\sqrt{k}} > \frac{4^{k+1}}{2\sqrt{k+1}}.$$

□

8.2. Упражнение. Доказать, что при $n \geqslant 1$ выполняется

$$\frac{4^n}{1+\sqrt{n}} \geqslant C_{2n}^n.$$

8.3. Лемма. $\theta(x) < (4 \ln 2)x$ при любом вещественном x.

Доказательство. В силу очевидных неравенств

$$4^n > C_{2n}^n > \prod_{\substack{n<p<2n \\ p-\text{простое}}} p$$

получаем $2n \ln 2 > \theta(2n) - \theta(n)$. Отсюда

$$\theta(2^m) \leqslant 2 \ln 2 (1 + 2 + \cdots + 2^{m-1}) < (2 \ln 2) 2^m,$$

и для $x = 2^m$ лемма верна. При $2^{m-1} < x < 2^m$ имеем

$$\theta(x) \leqslant \theta(2^m) < (2 \ln 2) 2^m = (4 \ln 2) 2^{m-1} < (4 \ln 2)x. \quad \square$$

8.4. Лемма. $\theta(n) > n/2$ при любом натуральном $n > 4$.

Доказательство. Для любого простого p обозначим через $\nu_p(n)$ максимальное k такое, что n делится на p^k. Оценим $\nu_p(n!)$. В произведении $1 \cdot 2 \cdot \ldots \cdot n$ на p делится ровно $\lfloor \frac{n}{p} \rfloor$ множителей, на p^2 – ровно $\lfloor \frac{n}{p^2} \rfloor$ и т.д. Поэтому

$$\nu_p(n!) = \sum_{i \geqslant 1} \Big\lfloor \frac{n}{p^i} \Big\rfloor.$$

Отсюда

$$\nu_p(C_{2n}^n) = \nu_p\Big(\frac{(2n)!}{(n!)^2}\Big) = \sum_{i \geqslant 1} \Big\lfloor \frac{2n}{p^i} \Big\rfloor - 2\sum_{i \geqslant 1} \Big\lfloor \frac{n}{p^i} \Big\rfloor$$

$$= \sum_{i \geqslant 1}^{i \leqslant \log_p(2n)} \Big(\Big\lfloor \frac{2n}{p^i} \Big\rfloor - 2\Big\lfloor \frac{n}{p^i} \Big\rfloor \Big) \leqslant \log_p(2n),$$

т.к. $\lfloor 2x \rfloor - 2\lfloor x \rfloor \leqslant 1$ для любого x. Далее,

$$C_{2n}^n = \prod_{p<2n} p^{\nu_p(C_{2n}^n)} \leqslant \prod_{p<2n} p^{\lfloor \log_p(2n) \rfloor}$$

$$\leqslant \prod_{p \leqslant \sqrt{2n}} p^{\log_p(2n)} \prod_{\sqrt{2n}<p\leqslant 2n} p^{\lfloor \log_p(2n) \rfloor} \leqslant (2n)^{(\sqrt{2n}+1)/2} \prod_{\sqrt{2n}<p\leqslant 2n} p.$$

Отсюда с помощью леммы 8.1 получаем

$$\theta(2n) > \sum_{\sqrt{2n}<p\leqslant 2n} \ln p \geqslant n \ln 4 - \ln 2 - \frac{1}{2}\ln n - \frac{1}{2}(\sqrt{2n}+1)\, \ln(2n).$$

Последняя функция больше n при $n \geqslant 134$ (проверьте это, например, с помощью программы Maple). Пусть $m \geqslant 268$. Тогда при m четном имеем $\theta(m) > m/2$. При m – нечетном имеем $\theta(m) = \theta(m+1) > (m+1)/2 > m/2$. Проверка того, что $\theta(m) > m/2$ при $4 < m < 268$ осуществляется с помощью программы. □

8.5. Следствие. Для любого натурального $n > 4$ произведение простых чисел, не превосходящих n, не менее $e^{n/2}$.

8.6. Замечания. 1) Пусть $\pi(x)$ обозначает количество простых чисел, не превосходящих x. В 1896 году Адамар и Валле-Пуссен независимо доказали, что $\lim\limits_{n\to+\infty} \frac{\pi(n)}{n/\ln n} = 1$. Последнее утверждение эквивалентно тому, что $\lim\limits_{n\to+\infty} \frac{\theta(n)}{n} = 1$.

2) Известно, что для любого натурального $n > 1$ произведение простых чисел из интервала $[n, 2n]$ больше 2^n.

Лекция 9

Полиномиальный детерминированный алгоритм распознавания простоты

9.1. Сравнения по модулю $(h(x), n)$**.** Для произвольного кольца K обозначим через $K[x]$ кольцо многочленов от x с коэффициентами из K. Пусть $h(x) \in \mathbb{Z}[x]$ и $n \in \mathbb{N}$. Говорят, что многочлены $f(x), g(x) \in \mathbb{Z}[x]$ сравнимы по модулю $(h(x), n)$ и пишут

$$f(x) \equiv g(x) \mod (h(x), n), \tag{9}$$

если существует $q(x) \in \mathbb{Z}[x]$ такой, что все коэффициенты многочлена $f(x)-g(x)-h(x)q(x)$ кратны n. Например,

$$x^3 + 3x^2 + 4x + 1 \equiv x + 1 \mod (x^2 + x + 1, 2).$$

Далее мы предполагаем, что старший коэффициент многочлена $h(x)$ равен 1. Для данного $f(x)$ всегда можно найти *остаток при делении на* $(h(x), n)$, т. е. такой многочлен $g(x)$, что выполнено сравнение (9), степень $g(x)$ меньше степени $h(x)$ и все коэффициенты многочлена $g(x)$ принадлежат множеству $\{0, 1, \ldots, n-1\}$. Для этого надо

1) разделив столбиком $f(x)$ на $h(x)$, найти такие многочлены $q(x)$ и $r(x)$, что $f(x) = h(x)q(x) + r(x)$, где степень $r(x)$ меньше степени $h(x)$;

2) в многочлене $r(x)$ заменить все коэффициенты их остатками при делении на n.

Легко понять, что остаток при делении $f(x)$ на $(h(x), n)$ единствен, а множество всех остатков, когда $f(x)$ пробегает $\mathbb{Z}[x]$, совпадает с множеством всех многочленов, степень которых меньше степени $h(x)$ и все их коэффициенты принадлежат множеству $\{0, 1, \ldots, n-1\}$.

Пусть F – множество всех возможных остатков при делении многочленов из $\mathbb{Z}[x]$ на $(h(x), n)$. Легко превратить F в кольцо, определив сумму (произведение) остатков $g_1(x)$ и $g_2(x)$ как остаток от деления $g_1(x)+g_2(x)$ (соответственно, $g_1(x)g_2(x)$) на $(h(x), n)$. Кольцо[5] F обозначают также $\mathbb{Z}_n[x]/\langle h(x)\rangle$. Остаток при делении $f(x)$ на $(h(x), n)$ назовем *образом* $f(x)$ *в* F.

Например, кольцо $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ состоит из остатков $0, 1, x, x + 1$, которые складываются и умножаются по следующим правилам:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Определение. Ненулевой многочлен $h(x) \in K[x]$ называется *неразложимым* в кольце $K[x]$, если из равенства $h(x) = h_1(x)h_2(x)$ следует, что $h_1(x) \in K$ или $h_2(x) \in K$.

Упражнение. 1) Проверьте, что многочлен $x^2 + x + 1$ неразложим в кольце $\mathbb{Z}_2[x]$, однако, разложим в кольце $\mathbb{Z}_3[x]$.

2) Докажите, что многочлен x^2+x+1 неразложим в кольце $\mathbb{Z}_p[x]$ для любого простого p при $p \equiv 2 \pmod 3$.

[5]Кольцо $\mathbb{F}$ изоморфно факторкольцу кольца $\mathbb{Z}_n[x]$ по идеалу, порожденному $h(x)$.

Лемма. Пусть n – простое число. Если многочлен $h(x) \in \mathbb{Z}[x]$ со старшим коэффициентом 1 неразложим в кольце $\mathbb{Z}_n[x]$, то кольцо $\mathbb{Z}_n[x]/\langle h(x)\rangle$ является полем.

Доказательство. Достаточно доказать, что в кольце $\mathbb{Z}_n[x]/\langle h(x)\rangle$ для любого его ненулевого элемента $g(x)$ существует обратный. Так как степень $g(x)$ меньше степени $h(x)$ и $h(x)$ неразложим в $\mathbb{Z}_n[x]$, то $\mathbf{нод}(g(x), h(x)) = 1$ в $\mathbb{Z}_n[x]$ и, как и в алгоритме Евклида для натуральных чисел, можно найти такие многочлены $u(x), v(x) \in \mathbb{Z}_n[x]$, что

$$g(x)u(x) + h(x)v(x) = 1.$$

Тогда $g(x)u(x) \equiv 1 \mod (h(x), n)$. Пусть $\overline{u}(x)$ – остаток при делении $u(x)$ на $(h(x), n)$. Тогда $g(x)\overline{u}(x) \equiv 1 \mod (h(x), n)$ и, значит, $\overline{u}(x)$ – обратный к $g(x)$ в кольце $\mathbb{Z}_n[x]/\langle h(x)\rangle$. □

9.2. Детская биномиальная теорема. Пусть n – натуральное число, $a \in \mathbb{Z}$ и $\mathbf{нод}(n, a) = 1$. Число n является простым тогда и только тогда, когда

$$(x+a)^n \equiv x^n + a \,(\bmod\, n). \tag{10}$$

Доказательство. Очевидно, что

$$(x+a)^n - (x^n + a) = \sum_{i=1}^{n-1} C_n^i x^i a^{n-i} + a^n - a. \tag{11}$$

Если n – простое, то C_n^i делится на n при $1 \leqslant i \leqslant n-1$. Кроме того, $a^n - a$ делится на n по малой теореме Ферма. Поэтому для простого n соотношение (11) выполняется.

Пусть теперь n составное, p – некоторый его простой делитель и p^k – максимальная степень p, входящая в разложение n. Тогда C_n^p делится на p^{k-1} и не делится на p^k и, значит, коэффициент при x^p в (11) не делится на n. Следовательно, при n составном соотношение (10) не выполняется. □

Для взаимно простых n и r обозначим через $\mathrm{ord}_r(n)$ порядок элемента n по модулю r, т.е. такое минимальное натуральное число $k \geqslant 1$, что $n^k \equiv 1 \,(\bmod\, r)$. Далее $\log n$ означает логарифм n по основанию 2.

9.3. Лемма. Для любого натурального $n > 4$ существует простое число $r \leqslant \log^5 n$, не делящее n, такое, что $\mathrm{ord}_r(n) > \log^2 n$.

Доказательство. Предположим, что для некоторого $n > 4$ выполняется противоположное: $\mathrm{ord}_r(n) \leqslant \log^2 n$ для любого простого r с условиями $r \nmid n$ и $r \leqslant m$, где $m = \lfloor \log^5 n \rfloor$. Тогда каждое такое r (а, значит, и их произведение) делит $\prod\limits_{1 \leqslant i \leqslant \log^2 n} (n^i - 1)$. Произведение простых r с условиями $r \mid n$ и $r \leqslant m$ не превосходит n. Отсюда и из следствия 8.5 получаем

$$2^{(\log e)m/2} = e^{m/2} \leqslant \prod_{\substack{r \leqslant m \\ r-\text{простое}}} r \leqslant n \cdot \prod_{1 \leqslant i \leqslant \log^2 n} (n^i - 1) < n^{1+1+2+\cdots+\lfloor \log^2 n \rfloor} \leqslant 2^{(\log^5 n + \log^3 n + 2\log n)/2}.$$

Противоречие. □

9.4. Теорема (Агравал, Кайал, Сахена, 2002 г). Пусть $n > 1$ – натуральное число, r – простое такие, что

(1) n не делится на простые числа $\leqslant r$;

(2) $\operatorname{ord}_r(n) > \log^2 n$;

(3) $(x+a)^n \equiv x^n + a \mod (x^r - 1, n)$ для всех $1 \leqslant a \leqslant A$, где $A = \sqrt{r}\log n$.

Тогда n – степень простого числа.

Доказательство. Пусть p – произвольный простой делитель n. Пусть $h(x)$ – неразложимый множитель $x^r - 1$ в кольце $\mathbb{Z}_p[x]$, отличный от $x-1$. Такой $h(x)$ существует, иначе $x^r - 1 = (x-1)^r$ в $\mathbb{Z}_p[x]$, тогда r делится на p, откуда $r = p$ – противоречие с условием (1). Так как $h(x)$ неразложим в кольце $\mathbb{Z}_p[x]$, то по лемме из пункта 9.1 кольцо $\mathbb{F} = \mathbb{Z}_p[x]/\langle h(x)\rangle$ является полем. Порядок элемента $x \in \mathbb{F}^*$ равен r, поскольку в $\mathbb{F}$ выполняется $x^r = 1$, $x \neq 1$ и r – простое.

Элементы $x, x+1, x+2, \ldots, x + \lfloor A \rfloor$ – ненулевые в $\mathbb{F}$. (Предположим, что $x + a = 0$ в $\mathbb{F}$. Тогда $x^n + a = (x+a)^n = 0$ в $\mathbb{F}$, и, значит, $x^n = -a = x$ в $\mathbb{F}$, откуда в силу $\operatorname{ord}(x) = r$ получаем $n \equiv 1 \pmod r$, т.е. $\operatorname{ord}_r(n) = 1$ – противоречие.) Пусть G – подмножество в $\mathbb{F}^*$, состоящее из всевозможных произведений этих элементов. По упражнению 3.8, G – циклическая подгруппа группы $\mathbb{F}^*$.

Любой многочлен $g(x) \in \mathbb{Z}[x]$ вида $g(x) = \prod\limits_{0\leqslant a\leqslant A} (x+a)^{e_a}$, где $e_a \geqslant 0$, представляет некоторый элемент из G. Поэтому $g(x)$ назовем G-многочленом. Для него имеем

$$g(x)^n = \prod_a ((x+a)^n)^{e_a} \equiv \prod_a (x^n + a)^{e_a} = g(x^n) \mod (x^r - 1,\, p).$$

Обозначим

$$I_{g(x)} = \{m > 0 \mid g(x)^m \equiv g(x^m) \mod (x^r - 1, p)\}.$$

Тогда $n, p \in I_{g(x)}$.

9.5. Лемма. Множество $I_{g(x)}$ замкнуто относительно умножения.

Доказательство. Пусть $m, k \in I_{g(x)}$. Имеем

$$g(x)^{mk} \equiv (g(x^m))^k \mod (x^r - 1, p).$$

С другой стороны, обозначая $y = x^m$, убеждаемся в равенстве

$$(g(x^m))^k \equiv g(x^{mk}) \mod (x^{mr} - 1, p).$$

Из него следует, что

$$(g(x^m))^k \equiv g(x^{mk}) \mod (x^r - 1, p).$$

Из этого и первого равенств вытекает, что $mk \in I_{g(x)}$. □

9.6. Лемма. Пусть $g(x)$ – G-многочлен, представляющий порождающий группы G. Тогда, если $m_1, m_2 \in I_{g(x)}$ и $m_1 \equiv m_2 \pmod r$, то $m_1 \equiv m_2 \pmod{|G|}$.

Доказательство. Пусть $m_2 = m_1 + kr$. Тогда в $\mathbb{F}$ имеем (учитывая, что $x^r = 1$ в $\mathbb{F}$)

$$g(x)^{m_1} g(x)^{kr} = g(x)^{m_2} = g(x^{m_2}) = g(x^{m_1+kr}) = g(x^{m_1}) = g(x)^{m_1}.$$

Так как $g(x) \neq 0$ в $\mathbb{F}$, то $g(x)^{kr} = 1$ в $\mathbb{F}$, откуда kr делится на порядок элемента $g(x)$, равный $|G|$. □

Пусть R – некоторое максимальное подмножество попарно несравнимых по модулю r чисел из множества $\{n^i p^j \mid i, j \geqslant 0\}$. Очевидно $|R| < r$. Кроме того, в силу леммы 9.5 имеем $R \subset I_{f(x)}$ для любого G-многочлена $f(x)$. Далее считаем, что p – наименьший простой делитель n.

Предположим, что n – не степень p.

Тогда целые числа $n^i p^j$ при $i, j \geqslant 0$ попарно различны. При $0 \leqslant i \leqslant \sqrt{|R|/2}$ и $0 \leqslant j \leqslant \sqrt{2\,|R|}$ имеется больше $|R|$ таких чисел, поэтому какие-то два из них должны совпадать по модулю r:

$$n^i p^j \equiv n^I p^J \,(\bmod\, r).$$

По лемме 9.5 оба этих числа лежат в $I_{g(x)}$, а по лемме 9.6 их разность делится на $|G|$. Отсюда

$$|G| \leqslant |n^i p^j - n^I p^J| < n^{\sqrt{|R|/2}} p^{\sqrt{2|R|}} < n^{\sqrt{2|R|}}.$$

Далее мы докажем, что $|G| > n^{\sqrt{2|R|}}$ и, тем самым, получим противоречие. Из этого будет следовать, что n является степенью p.

9.7. Лемма. Пусть $f_1(x), f_2(x)$ – G-многочлены из $\mathbb{Z}[x]$ степени $< |R|$. Предположим, что их образы в $\mathbb{F}$ совпадают, т.е. $f_1(x) \equiv f_2(x) \mod (h(x), p)$. Тогда $f_1(x) = f_2(x)$ в $\mathbb{Z}_p[x]$.

Доказательство. Так как $R \subset I_{f_i(x)}$ для $i = 1, 2$, то для любого $k \in R$ справедливо

$$f_i(x^k) \equiv f_i(x)^k \mod (h(x), p).$$

Отсюда и из условия вытекает, что

$$f_1(x^k) \equiv f_2(x^k) \mod (h(x), p).$$

Далее, при разных $k \in R$ элементы $x^k \in \mathbb{F}$ различны. Это вытекает из того, что числа из R попарно несравнимы по модулю r и $\operatorname{ord}(x) = r$ в $\mathbb{F}^*$. Поэтому многочлены f_1 и f_2 степени $< |R|$ имеют одинаковые значения в поле $\mathbb{F}$ на $|R|$ элементах этого поля. Значит их коэффициенты при одинаковых степенях x совпадают в поле $\mathbb{F}$, т.е. дают одинаковые остатки при делении на p. $\square$

• Докажем, что $|G| > n^{\sqrt{2|R|}}$. Можно считать, что числа $1, n, \ldots, n^{\operatorname{ord}_r(n)-1}$ входят в R. Поэтому $|R| \geqslant \operatorname{ord}_r(n) > \log^2 n$ и, значит, $|R| > B$, где $B = \lfloor \sqrt{|R|} \log n \rfloor$. Кроме того, $A \geqslant B$, где A из условия (3).

Рассмотрим G-многочлены $g(x) = \prod\limits_{0 \leqslant a \leqslant B} (x+a)^{e_a}$ с условием $\sum\limits_{0 \leqslant a \leqslant B} e_a = B$. Их количество равно числу разбиений числа B на $B+1$ слагаемых, т.е. C_{2B}^B. Их корни со знаком минус неотрицательны и не превосходят p, поскольку $B < |R| < r < p$. Поэтому эти многочлены имеют разные наборы корней по модулю p при разных наборах показателей e_a. Значит эти многочлены различны в кольце $\mathbb{Z}_p[x]$. По лемме 9.7 их образы в $\mathbb{F}$ различны. Так как эти образы лежат в G, то с учетом леммы 8.1 получаем

$$|G| \geqslant C_{2B}^B \geqslant \frac{4^B}{2B^{1/2}} > \frac{4^{\sqrt{|R|}\log n - 1}}{2p^{1/2}} > \frac{n^{2\sqrt{|R|}}}{8n^{1/4}}. \tag{12}$$

Так как n – не степень простого, то $n \geqslant 6$. Учитывая неравенство $|R| > \log^2 n$, с помощью программы можно вывести, что последнее выражение в (12) больше $n^{\sqrt{2|R|}}$ при $n \geqslant 6$. Теорема доказана. $\square$

9.10. Детерминированный тест на простоту (Агравал, Кайал, Сахена.) Пусть $n > 1$ – натуральное число. Обозначим $m = \lfloor \log^5 n \rfloor$. При $n < 5690034$ проверка простоты осуществляется с помощью решета Эратосфена. При $n > 5690034$ выполняется $n > m$. В этом случае делаются следующие шаги.

(1) Проверить, делится ли n на натуральные числа от 2 до m.

(2) Найти простое число $r \leqslant m$ такое, что $\mathrm{ord}_r(n) > \log^2 n$.

(3) Проверить выполняется ли сравнение

$$(x+a)^n \equiv x^n + a \mod (x^r - 1, n)$$

для всех $1 \leqslant a \leqslant A$, где $A = \sqrt{r} \log n$.

(4) Проверить, существует ли натуральное $l \geqslant 2$ такое, что $n = q^l$ для некоторого натурального q.

Если на шаге (1) число n делится на некоторое натуральное число из интервала $[2, m]$, то n составное. Если n не делится на все числа из этого интервала, то переходим к шагу (2). Согласно лемме 9.3 искомое число r существует и его можно найти перебором. Далее переходим к шагу (3). Если указанное сравнение не выполняется хотя бы для одного a из интервала $1 \leqslant a \leqslant A$, то n составное (по теореме 9.2). Если выполняется, то n – степень простого (по теореме 9.4). В этом случае шаг (4) завершает тест.

9.11. Полиномиальность алгоритма Агравала-Кайала-Сахены. Указанный алгоритм проверяет простоту n за полиномиальное число операций от $\lfloor \log n \rfloor$. Под операциями понимаются сложение и умножение чисел, не превосходящих n, по модулям, не превосходящим n, а также вычисление остатков таких чисел[6].

Поясним лишь, как можно быстро вычислить остатки при делении $x^n + a$ и $(x+a)^n$ на $(x^r - 1, n)$. Первый остаток равен $x^s + a$, где s – остаток при делении n на r. Второй остаток вычисляется с помощью следующего замечания.

Пусть $f(x)$ и $g(x)$ – произвольные остатки при делении на $(x^r - 1, n)$, т.е. $f(x)$ и $g(x)$ – многочлены степени не более r, с коэффициентами из множества $\{0, 1, \ldots, n-1\}$. Тогда остаток при делении $f(x)g(x)$ на $(x^r - 1, n)$ ищется с помощью не более, чем r^2 умножений, r сложений и вычисления r остатков при делении чисел на n. Назовем совокупность этих операций блок-шагом. В частности, остаток при делении $f(x)^2$ на $(x^r - 1, n)$ ищется за один блок-шаг.

Поэтому при $n = 2^l$ остаток при делении $(x+a)^n$ на $(x^r - 1, n)$ ищется за $l = \log n$ блок-шагов. В общем случае, при $n = 2^{l_1} + 2^{l_2} + \cdots + 2^{l_k}$, где $l_1 > l_2 > \cdots > l_k$, остаток ищется за не более, чем $2\lfloor \log n \rfloor$ блок-шагов (докажите!).

9.12. Упражнение. 1) Запрограммировать алгоритм из пункта 9.10.

2) Проверить, что число 1111111111111111111 – простое. Чему равно минимальное r из шага (2)?

9.13. Замечание. С 2002 года появилось несколько модификаций и улучшений алгоритма Агравала-Кайала-Сахены. Доказанная на сегодняшний момент оценка сложности этого алгоритма: $O(\log^{7,5} n)$ битовых операций. На практике число r находится быстро вблизи числа $\log^2 n$. Основная сложность алгоритма заключена в шаге (3). В работе [**?**] приведена гипотеза, сводящая $\lfloor A \rfloor$ проверок на шаге (3) к одной.

[6]Монтгомери предложил быстрый алгоритм умножения чисел по модулю n, см., например, [**?**].

Лекция 10
Построение больших простых чисел

10.1. Кольцо $\mathbb{Z}_n[\sqrt{q}\,]$. Пусть n – натуральное число, q – целое, $q \neq 0, 1$ и q не делится на квадрат натурального числа, отличного от 1. Рассмотрим множество всех выражений вида $a + b\sqrt{q}$, где a, b пробегают кольцо вычетов $\mathbb{Z}_n$. Эти выражения можно естественным способом складывать и перемножать. Например, если $n = 5, q = 3$, то

$$(2+\sqrt{3})(3+4\sqrt{3}) = 0+0\sqrt{3} \quad \text{и} \quad (2+\sqrt{3})(3+4\sqrt{3}) = 3+\sqrt{3}.$$

Легко доказать, что таким образом получается кольцо с нулем $0+0\sqrt{q}$ и единицей $1+0\sqrt{q}$. Обозначим это кольцо через $\mathbb{Z}_n[\sqrt{q}\,]$. *Нормой* элемента $a + b\sqrt{q}$ этого кольца называется элемент $a^2 - qb^2$ кольца $\mathbb{Z}_n$; обозначается норма через $N(a + b\sqrt{q})$.

Упражнение. 1) Доказать, что норма произведения двух элементов кольца $\mathbb{Z}_n[\sqrt{q}\,]$ равна произведению их норм.

2) Доказать, что элемент кольца $\mathbb{Z}_n[\sqrt{q}\,]$ обратим тогда и только тогда, когда его норма обратима в кольце $\mathbb{Z}_n$.

3) Найти порядок группы обратимых элементов кольца $\mathbb{Z}_5[\sqrt{3}\,]$.

10.2. Числа Мерсенна. *Числом Мерсенна* называется любое натуральное число вида $2^n - 1$.

Заметим, что в двоичной записи число $2^n - 1$ записывается n единицами.

Очевидно, если $M_n = 2^n - 1$ – простое, то n – тоже простое. Обратное неверно: $2^{11} - 1 = 23 \cdot 89$. На сей момент известно 43 простых числа Мерсенна. Первые 12 из них (при $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$) открыты до 1887 года, следующее (при $n = 521$) – только в 1952 году. Последнее, $M_{30402457}$ открыто в 2005 году с помощью совместных вычислений многих компьютеров в сети Internet. Оно является также наибольшим известным на данный момент простым числом.

Для изучения простых чисел Мерсенна определим последовательность Люка $S_1, S_2, \ldots$ по правилу: $S_0 = 2$, $S_1 = 4$ и $S_{n+1} = 4S_n - S_{n-1}$. Определим еще одну последовательность: $L_1 = 4$, $L_{n+1} = L_n^2 - 2$.

Упражнение. Пусть $u = 2 + \sqrt{3}$, $v = 2 - \sqrt{3}$. Доказать формулы

1) $u^{n+1} = 4u^n - u^{n-1}$, $v^{n+1} = 4v^n - v^{n-1}$;
2) $S_n = u^n + v^n$;
3) $L_n = u^{2^{n-1}} + v^{2^{n-1}}$;
4) $L_n = S_{2^{n-1}}$.

10.3. Теорема (Люка-Лемер). Пусть $n > 2$. Число $M_n = 2^n - 1$ – простое тогда и только тогда, когда L_{n-1} делится на $2^n - 1$.

Доказательство. По упражнению из п. 10.2 имеем

$$L_{n-1} = u^{2^{n-2}} + v^{2^{n-2}}.$$

Предположим, что L_{n-1} делится на M_n. Тогда

$$u^{2^{n-2}} + v^{2^{n-2}} = kM_n.$$

Умножая на $u^{2^{n-2}}$, получаем

$$u^{2^{n-1}} = kM_n u^{2^{n-2}} - 1.$$

Предположим, что число M_n – составное. Тогда оно имеет простой делитель $r \leqslant \sqrt{M_n}$. Рассмотрим последнее равенство, как равенство в кольце $\mathbb{Z}_r[\sqrt{3}\,]$. Тогда $u^{2^{n-1}} = -1$ в этом кольце. Поэтому порядок элемента u в группе обратимых элементов этого кольца равен 2^n. Так как порядок этой группы не превосходит $r^2 - 1$, то

$$2^n \leqslant r^2 - 1 < M_n.$$

Противоречие.

Предположим теперь, что $p = 2^n - 1$ – простое число. Покажем, что $S_{2^{n-1}} \equiv -2 \,(\bmod p)$. Тогда будет выполняться $L_n \equiv -2 \,(\bmod p)$, а значит, $L_{n-1} \equiv 0 \,(\bmod p)$, что и требуется доказать. Справедливо равенство

$$2 \pm \sqrt{3} = \Big(\frac{\sqrt{2} \pm \sqrt{6}}{2}\Big)^2.$$

Тогда по упражнению из п. 10.2 получаем

$$S_{2^{n-1}} = \Big(\frac{\sqrt{2} + \sqrt{6}}{2}\Big)^{p+1} + \Big(\frac{\sqrt{2} - \sqrt{6}}{2}\Big)^{p+1} =$$

$$2^{-p} \sum_{0 \leqslant k \leqslant \frac{p+1}{2}} C_{p+1}^{2k} (\sqrt{2}\,)^{p+1-2k} (\sqrt{6}\,)^{2k} =$$

$$2^{\frac{p+1}{2} - p} \sum_{0 \leqslant k \leqslant \frac{p+1}{2}} C_{p+1}^{2k} \cdot 3^k =$$

$$2^{\frac{1-p}{2}} \sum_{0 \leqslant k \leqslant \frac{p+1}{2}} C_{p+1}^{2k} \cdot 3^k.$$

Так как p – нечетное простое число, то C_{p+1}^{2k} делится на p при всех k, кроме $k = 0$ и $k = \frac{p+1}{2}$. Следовательно,

$$2^{\frac{p-1}{2}} S_{2^{n-1}} \equiv 1 + 3^{\frac{p+1}{2}} \,(\bmod p).$$

По предположению число $p = 2^n - 1$ – простое и $n > 2$. Поэтому n нечетно и, значит, $p \equiv 1 \,(\bmod 3)$, в частности, $\left(\frac{p}{3}\right) = 1$. Тогда из квадратичного закона взаимности Гаусса следует, что

$$3^{\frac{p-1}{2}} \equiv \left(\frac{3}{p}\right) \equiv (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{3}\right) \equiv -1 \,(\bmod p).$$

Поэтому

$$2^{\frac{p-1}{2}} S_{2^{n-1}} \equiv 1 + 3 \cdot (-1) \equiv -2 \,(\bmod p).$$

Далее, $p = 2^n - 1 \equiv -1 \,(\bmod 8)$, откуда

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv 1 \,(\bmod p).$$

В итоге $S_{2^{n-1}} \equiv -2 \,(\bmod p)$, что мы и хотели доказать. □

10.4 Упражнение. 1) Напишите программу, проверяющую числа вида $2^n - 1$ на простоту с помощью теоремы Люка-Лемера.
2) Оцените число битовых операций, необходимых для проверки числа $2^n - 1$ на простоту.
3) Проверьте, что число Мерсенна M_{521} простое.

Список литературы

[1] О.Н. Василенко, *Теоретико-числовые алгоритмы в криптографии*, М.: МЦНИМО, 2003.

[2] Н. Смарт, *Мир программирования и криптографии*, перевод с англ., М.: Техносфера, 2005.

[3] А.В. Черемушкин, *Лекции по арифметическим алгоритмам в криптографии*, М.: МЦНИМО, 2002.

[4] Введение в криптографию (ред. Ященко), М.: МЦНИМО, 2000.

[5] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in NP*, 2004.

[6] E. Bach and J. Shallit, *Algorithmic number theory*, v. I: Efficient algorithms, MIT Press, Cambridge – Massachusetts, 1996.

[7] A. Granville, *It is easy to determine whether a given integer is prime*, Bulletin of the American Math. Soc., v. 42, N 1, 3-38.

[8] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, Cambridge, 2005. Available on the website http://www.shoup.net/ntb.