Домашнее задание по теории чисел

Количество баллов за каждую задачу указано в скобках после номера задачи. Если вы обнаружите опечатки в формулировках задач, пожалуйста, сообщите об этом по адресу m.vsemirnov@gmail.com

Делимость.

Определение. Пусть a, b — целые числа. Говорим, что a делится на b (b делит a, если существует $c \in \mathbb{Z}$, такое, что $a = bc$.

Обозначения.

$a \vdots b$ — a делится на b;
$b \mid a$ — b делит a;

$a \not\vdots b$ — a не делится на b;
$b \nmid a$ — b не делит a.

Свойства.
1. Если $b \mid a_1$, $b \mid a_2$, то $b \mid (a_1 \pm a_2)$.
2. $b \mid b$.
3. Если $b \mid a$, $c \mid b$, то $c \mid a$.
4. Если $a, b \in \mathbb{Z}$, $b \mid a$, $a \mid b$, то $a = \pm b$.

Задача 1. [1] Проверьте свойства делимости.

Наибольший общий делитель.

Определение. Пусть $a_1,\ldots,a_n$ — целые числа. Наибольшим общим делителем чисел $a_1,\ldots,a_n$ называется целое d, такое, что
1. $d \mid a_1,\ldots,d \mid a_1$;
2. для всякого d_1 такого, что $d_1 \mid a_1,\ldots,d_1 \mid a_1$, выполнено $d_1 \mid d$.

Обозначения. НОД$(a_1, \ldots, a_n)$, $\gcd(a_1, \ldots, a_n)$ (greatest common divisor).

Определение. Непустое подмножество I множества целых чисел называется идеалом в $\mathbb{Z}$, если
1. $\forall a, b \in I$ $[a \pm b \in I]$.
2. $\forall a \in I$ $\forall r \in \mathbb{Z}$ $[ra \in I]$.

(В случае $\mathbb{Z}$ свойство 2 следует из свойства 1, однако определение дается в таком виде, чтобы оно было согласовано с определением идеала в произвольном коммутативном кольце.)

Определение. Наименьший идеал, содержащий $a_1, \ldots, a_n$ называется идеалом, порожденным $a_1, \ldots, a_n$, и обозначается $(a_1, \ldots, a_n)$.

Задача 2. [1] Докажите, что $(a_1, \ldots, a_n) = \{x_1a_1 + \cdots + x_na_n : x_1, \ldots, x_n \in \mathbb{Z}\}$.

Определение. Идеал, порожденный одним элементом, называется главным.

Задача 3. [1] Докажите, что $a \mid b$ в $\mathbb{Z}$, тогда и только тогда, когда $(b) \subseteq (a)$.

Задача 4. [1] Докажите, что в $\mathbb{Z}$ все идеалы главные. (Указание: если идеал I отличен от $\{0\}$, то рассмотрите наименьшее натуральное число, ему принадлежащее, и примените лемму о делении с остатком.)

Свойства НОД.
1. В $\mathbb{Z}$ НОД определен однозначно с точностью до знака.
2. В $\mathbb{Z}$ имеет место равенство идеалов $(d) = (a_1, \ldots, a_n)$, тогда и только тогда, когда $d = \gcd(a_1, \ldots, a_n)$.
3. Для любых целых $a_1, \ldots, a_n$, существует $\gcd(a_1, \ldots, a_n)$.
4. Для любых целых $a_1, \ldots, a_n$, наибольший общий делитель $d = \gcd(a_1, \ldots, a_n)$ допускает линейное представление $d = x_1a_1 + \cdots + x_na_n$ для некоторых целых $x_1,\ldots,x_n$.
5. Если $a = bq + r$, то $(a, b) = (b, r)$.
6. $(a, 0) = (a)$.

Задача 5. [1] Докажите перечисленные выше свойства НОД.

Алгоритм Евклида.

Пусть a, $b \in \mathbb{Z}$. Положим $a_0 = a$, $a_1 = b$ и рекурсивно определим последовательность a_i: $a_{i-2} = a_{i-1}q_{i-1} + a_i$, $0 \le a_i < |a_{i-1}|$, $i = 2, \ldots$.

Задача 6. [1] Докажите, что а) описанный выше алгоритм завершает работу за конечное число шагов; б) если $a_n = 0$, то $a_{n-1} = \gcd(a, b)$.

Линейное представление НОД также можно находить при помощи алгоритма Евклида. Положим $u_0 = 1$, $u_1 = 0$, $v_0 = 0$, $v_1 = 1$, $u_i = u_{i-2} - q_{i-1}u_{i-1}$, $v_i = v_{i-2} - q_{i-1}v_{i-1}$, $i = 2, \ldots$.

Задача 7. [1] Покажите, что $a_i = u_ia + v_ib$. В частности, в обозначениях задачи 6, $a_{n-1} = u_{n-1}a + v_{n-1}b$ — линейное представление $\gcd(a, b)$.

Задача 8. [1] Найдите наибольший общий делитель чисел 635226744 и 1453306515 и его линейное представление.

Задача 9. [1] а) Покажите, что в алгоритме Евклида $a_{i+2} < a_i/2$. Выведите отсюда, что число арифметических операций, необходимых для выполнения алгоритма Евклида есть $O(\log_2(\max\{|a|, |b|\}))$. б) Покажите, что число двоичных операций в алгоритме Евклида можно оценить сверху величиной $O((\log_2(\max\{|a|, |b|\}))^3)$ (предполагается, что умножение, деление, сложение, вычитание выполняются обычным способом "в столбик").

Задача 10. [1] Определим числа Фибоначчи равенствами $F_0 = 0$, $F_1 = 1$, $F_i = F_{i-1} + F_{i-2}$. а) Пусть $a > b > 0$ и алгоритм Евклида для пары (a, b) требует n шагов. Покажите, что $a \ge F_{n+2}$. б) Пользуясь результатом пункта а), найдите оптимальную постоянную в символе O из задачи 9а.

Задача 11. [1] а) Покажите, что деление с остатком $a = qb + r$, $0 \le r < |b|$ требует $O(\log_2 b \cdot (1 + \log_2 q))$ двоичных операций. б) Применяя эту оценку к каждому шагу алгоритма Евклида, улучшите оценку из задачи 9б), показав, что алгоритм требует $O(\log_2 a \cdot \log_2 b)$ двоичных операций.

Задача 12. [1] а) Оцените число двоичных операций, необходимых для нахождения линейного представления НОД по алгоритму Евклида.

Задача 13. [1] (Модифицированный алгоритм Евклида). Оцените число шагов для версии алгоритма Евклида, в которой на каждом шаге выбирается наименьший по абсолютной величине остаток: $a_{i-2} = a_{i-1}q_{i-1} + a_i$, $|a_{i-1}|/2 \le a_i < |a_{i-1}|/2$, $i = 2, \dots$.

Задача 14. [1] (Бинарный алгоритм Евклида). а) Рассмотрите алгоритм нахождения НОД основанный на следующей рекурсивной процедуре:

1) $\gcd(a, b) = \gcd(b, a) = \gcd(|a|, |b|)$;
2) $\gcd(a, a) = a$;
3) если a, b четны, то $\gcd(a, b) = 2\gcd(a/2, b/2)$;
4) если a четно, а b нечетно, то $\gcd(a, b) = \gcd(a/2, b)$;
5) если a нечетно, а b четно, то $\gcd(a, b) = \gcd(a, b/2)$;
6) если a, b нечетны, $a > b > 0$, то $\gcd(a, b) = \gcd(a - b, b)$.

Покажите, что число двоичных операций, требуемых для нахождения НОД при помощи этого алгоритма, есть $O((\log_2 a)^2)$.

б) Чем этот алгоритм удобен для машинной реализации?

в) Почему этот алгоритм в приведенном виде не всегда лучше классического алгоритма Евклида?

Задача 15. [1] Пусть $a \ge 2$ — целое число. Найдите $\gcd(a^n - 1, a^m - 1)$.

Задача 16. [1] Пусть $a \ge 2$ — целое число. Найдите $\gcd(a^n + 1, a^m + 1)$.

Задача 17. [1] Пусть a — целое число. Найдите $\gcd(a^2 + 1, 2a + 3)$.

Взаимно простые числа

Числа $a_1, \dots, a_n$ называются взаимно простыми, если $\gcd(a_1, \dots, a_n) = 1$.

Задача 18. [1] Докажите, что $a_1, \dots, a_n$ взаимно просты тогда и только тогда, когда существуют целые $x_1, \dots, x_n$, такие, что $a_1x_1 + \dots + x_na_n = 1$.

Задача 19. [1] Пусть $\gcd(a_1, \dots, a_n) = d$. Докажите, что $a_1/d, \dots, a_n/d$ взаимно просты.

Задача 20. [1] а) Докажите, что если каждое из чисел $a_1, \dots, a_n$ взаимно просто с n, то и $a_1 \cdots a_n$ взаимно просто с n.

б) Даны целые числа $a_1, \dots, a_n$, $b_1, \dots, b_m$. Известно, что для всех $1 \le i \le n$, $1 \le j \le m$ числа a_i и b_j взаимно просты. Докажите, что $a_1 \cdots a_n$ и $b_1 \cdots b_m$ взаимно просты.

Задача 21. [1] Пусть $n \mid ab$ и $\gcd(n, a) = 1$. Докажите, что $n \mid b$. (Указание: воспользуйтесь линейным представлением $\gcd(n, a)$.)

Линейные диофантовы уравнения

Задача 22. [1] а) Пусть a, b, c — фиксированные целые числа. Докажите, что уравнение $ax + by = c$ разрешимо в целых числах x и y тогда и только тогда $\gcd(a, b) \mid c$. б) Покажите, что если $ax_0 + by_0 = c$, то решениями уравнения $ax + by = c$ в целых числах будут пары $(x, y) = (x_0 + tb/\gcd(a, b), y_0 - ta/\gcd(a, b))$, $t \in \mathbb{Z}$, и только они.

Задача 23. [1] Сколькими способами число 123456789 можно представить в виде суммы двух положительных слагаемых, первое из которых делится на 11, а второе делится на 101?

Задача 24. [1] Решите уравнение $24x - 63y + 98z + 5 = 0$ в целых числах.

Простые и составные числа. Основная теорема арифметики.

Целое число n ($|n| > 1$) называется простым, если все его делители — это ± 1, $\pm n$. Целое число n ($|n| > 1$) называется составным, если у него имеется делитель — это ± 1, $\pm n$.

Задача 25. [1] Докажите, что всякое ненулевое целое число n можно представить в виде $n = \varepsilon p_1 \cdots p_k$, где $\varepsilon = \pm 1$, а все p_i — положительные простые числа, причем такое представление единственно с точность до порядка сомножителей.

Задача 26. [1] Пусть $s \ge 1$. Покажите, что

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

где произведение берется по всем простым. Выведите отсюда, что простых чисел бесконечно много.

Задача 27. [1] а) Докажите, что аддитивная группа $(\mathbb{Q}, +)$ порождается всеми дробями вида $\frac{1}{p^k}$, где p пробегает все простые числа, а k пробегает все натуральные. б) Докажите, что у этой группы нет конечной системы образующих.

Пусть p — простое число. На множестве ненулевых целых чисел определим функцию ord_p: если $n = p^k \cdot a$, $\gcd(a, p) = 1$, то $\mathrm{ord}_p(n) = k$.

Задача 28. [1] Докажите, что $\mathrm{ord}_p(nm) = \mathrm{ord}_p(n) + \mathrm{ord}_p(m)$.

Задача 29. [1] Найдите $\mathrm{ord}_p(n!)$.

Задача 30. [1] Докажите, что $\mathrm{ord}_p\left(\binom{a+b}{a}\right)$ есть число переносов из разряда в разряд при сложении a и b в p-ичной системе счисления (теорема Куммера).

Сравнения

Пусть $m \ne 0$ — фиксированное целое число. Рассмотрим следующее отношение на множестве целых чисел:

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b).$$

Читается: “a сравнимо с b по модулю m”.

Задача 31. [1] Докажите, что отношение сравнимости является отношением эквивалентности на множестве целых чисел. Опишите классы эквивалентности.

Свойства сравнений:
1. Если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $a + c \equiv b + d \pmod m$, $a - c \equiv b - d \pmod m$.
2. Если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $ac \equiv bd \pmod m$.
3. Если $n \in \mathbb{N}$ и $a \equiv b \pmod m$ то $a^n \equiv b^n \pmod m$.
4. Если $a \equiv b \pmod m$ и $n \mid m$, то $a \equiv b \pmod n$.
5. Если $n \in \mathbb{Z}$ и $a \equiv b \pmod m$ то $an \equiv bn \pmod{nm}$.
6. Если $n \in \mathbb{Z}$, $na \equiv nb \pmod m$ и $\gcd(n, m) = 1$, то $a \equiv b \pmod m$.
7. Если $n \in \mathbb{Z}$, $na \equiv nb \pmod m$ и $d = \gcd(n, m)$, то $a \equiv b \pmod{m/d}$.

Задача 32. [1] Докажите эти свойства сравнений. Покажите, что в свойстве 6 предположение о взаимной простоте n и m существенно.

Задача 33. [1] Пусть a, b, $m \in \mathbb{Z}$. Докажите, что сравнение $ax = b \pmod m$ разрешимо, тогда и только тогда, $\gcd(a, m) \mid b$.

Задача 34. [1] Решите сравнения: а) $37x \equiv 5 \pmod{51}$; б) $11x \equiv 5 \pmod{341}$; в) $65x \equiv 39 \pmod{1092}$;

Малая теорема Ферма. Теорема Эйлера. Числа Кармайкла

Пусть $\varphi(n)$ — количество чисел от 1 до n и взаимно простых с n.

В задачах 35г,д, 36 можно применять компьютер. Достаточно предъявить ответ и распечатку программы.

Задача 35. [2] а) Пусть p — простое число. Докажите, что если $\gcd(a, p) = 1$, то числа a, $2a$,…,$(p-1)a$ попарно несравнимы по модулю p. Выведите отсюда, что $a^{p-1} \equiv 1 \pmod p$ (малая теорема Ферма).

б) Если $\gcd(a, n) = 1$ и $a^{n-1} \not\equiv 1 \pmod n$, то n — составное число.

в) Вычислите $2^{1146} \pmod{1147}$. Пользуясь этим результатом, покажите, что число 1147 составное.

г) Найдите наименьшее составное число n, такое, что $2^{n-1} \equiv 1 \pmod n$. Найдите все такие составные числа, меньшие 1000.

д) Найдите наименьшее составное число n, такое, что $2^{n-1} \equiv 1 \pmod n$ и $2^{n-1} \equiv 1 \pmod n$. Найдите все такие составные числа, меньшие 1000.

Задача 36. [1] Найдите составное число n, такое, $a^{n-1} \equiv 1 \pmod n$ для всех целых a взаимно простых с n. Такие n называются числами Кармайкла. Найдите все числа Кармайкла, меньшие 1000.

Задача 37. [1] а) Докажите, что если $\gcd(a, n) = 1$, а a_1,…,$a_{\varphi(n)}$ — взаимно просты с n и попарно несравнимы по модулю n, то числа aa_1, aa_2,…,$aa_{\varphi(n)}$ также взаимно просты с n и попарно несравнимы по модулю p. Выведите отсюда, что $a^{\phi(n)} \equiv 1 \pmod n$ (Теорема Эйлера).