Малая теорема Ферма. Составитель А. Скопенков.

Латинские буквы обозначают целые числа. Буквы p и q обозначают простые числа. Из задач 1 и 2 достаточно сдать последний пункт.

1. (a) Имеет ли решения уравнение $13x \equiv 2005 \pmod{17}$?

(b) Пусть $Z_{17} = \{0, 1, \dots, 16\}$. Рассмотрим отображение $f\colon Z_{17} \to Z_{17}$, заданное так: $f(a)$ равно остатку от деления числа $13a$ на 17. Тогда f — биекция.

(c) Сформулируйте и докажите аналог предыдущего пункта для произвольного p.

2. (a) $(13 \cdot 1) \cdot (13 \cdot 2) \cdot \ldots \cdot (13 \cdot 16) \equiv 16! \pmod{17}$. (b) $13^{16} \equiv 1 \pmod{17}$.

(c) *Малая теорема Ферма.* Если p простое, то $n^p - n$ делится на p для любого целого n.

3. (a) Число $\underbrace{11\ldots1}_{2002}$ делится на 2003.

(c)* Верна ли теорема, обратная к малой теореме Ферма?

4. (a) $p-1$ делится на наименьшее $k > 0$, для которого $a^k \equiv 1$ (p).

(b) Длина периода десятичной дроби $1/p$ делит $p-1$.

(c) Если $p > 2$ и $2^p - 1$ делится на q, то $q-1$ делится на $2p$.

5. (a) Если $p \neq q$ и n не делится ни на p, ни на q, то $n^{(p-1)(q-1)} - 1$ делится на pq.

(b) Если n не делится на p, то $n^{p^k(p-1)} - 1$ делится на p^{k+1}.

(c) Если n взаимно просто с $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ и $\varphi(m) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{\alpha_k - 1}$, то $n^{\varphi(m)} - 1$ делится на m.

(d) $\varphi(m)$ равно количеству чисел от 1 до m, взаимно простых с m.

(e) Известно, что n — нечетное число от 3 до 47, не делящееся на 5. Как быстро вычислять неизвестное n по известному n^7 mod50?

Квадратичный закон взаимности. Составитель А. Скопенков.

1. (a) Выясните, какие остатки могут давать квадраты натуральных чисел при делении на 3,4,5,6,7,8,9,10.

(b) Если $a^2 + b^2$ делится на 3 (на 7), то a и b делятся на 3 (на 7).

(c) Число вида $4k + 3$ не представимо в виде суммы двух квадратов.

(d) Число, имеющее простой делитель вида $4k + 3$ в нечетной степени, не представимо в виде суммы двух квадратов.

(e)* Остальные целые числа представимы в виде суммы двух квадратов.

(f) Существуют сколь угодно большие тройки последовательных натуральных чисел, ни одно из которых не является точным квадратом.

2. Решите уравнения в целых числах.

(a) В нечетных числах: $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = y^2$. (b) $x^2 + y^2 = 3z^2$.

(c) $x^2 = 83y - 1$. Указание: используйте малую теорему Ферма.

(d) $x^2 + 1 = py$, где p — простое и $p \equiv 3 \pmod{4}$.

3. Сведите уравнение $py = at^2 + bt + c$ к сравнению $x^2 \equiv a$ (p).

Соглашения: $p > 2$ – простое число; латинские буквы обозначают целые числа или остатки (что именно — видно из контекста).

Остаток $a \neq 0$ называется *квадратичным вычетом (квадратичным невычетом) по модулю* p, если сравнение $x^2 \equiv a(p)$ разрешимо (неразрешимо). Слова 'по модулю p' далее всюду опускаются.

4. (a) Сравнение $x^2 \equiv a^2(p)$ имеет ровно два решения для a, не делящегося на p.

(b) Число квадратичных вычетов равно числу квадратичных невычетов и равно $\frac{p-1}{2}$.

5. (a) Для любого $a \neq 0$ существует и единственно a^{-1}, такое что $aa^{-1} \equiv 1(p)$.

(b) Решите сравнение $x \equiv x^{-1}(p)$.

(c) *Теорема Вильсона.* $(p-1)! + 1$ делится на p.

6. (a) Если $a \neq 0$ квадратичный вычет, то a^{-1} тоже квадратичный вычет.

(b) Число квадратичных вычетов четно тогда и только тогда, когда -1 является квадратичным вычетом.

(c) Уравнение $x^2+1=py$ разрешимо в целых числах при $p\equiv 1(4)$.

7. (a) Произведение двух квадратичных вычетов является квадратичным вычетом.

(b) Произведение квадратичного вычета и квадратичного невычета является квадратичным невычетом.

(c) Произведение двух квадратичных невычетов является квадратичным вычетом.

8. Если число $p=8k+5$ простое, то

(a) $2^{4k+2}\equiv -1(p)$.

(b) уравнение $x^2-2=py$ неразрешимо в целых числах.

9. (a) Многочлен степени n над Z_p имеет не более n корней.

(b)* *Критерий Эйлера.* $a^{\frac{p-1}{2}}\equiv (\frac{a}{p}):\equiv \begin{cases} +1, & a \text{ квадратичный вычет по модулю } p \\ -1, & a \text{ квадратичный невычет по модулю } p \end{cases}$.

10. (a) Если число $p=8k+1$ простое, то $2^{4k}\equiv 1\ (p)$.

(b) Если число $p=8k+1$ простое, то уравнение $x^2-2=py$ разрешимо в целых числах.

(c) Для каких простых p разрешимо в целых числах уравнение $x^2-2=py$?

(d)* А уравнение $x^2-3=py$?

11. (a) $(\frac{a}{p})\equiv(-1)^{\sum\limits_{x=1}^{(p-1)/2}[\frac{2ax}{p}]}\ (p)$.

(b)* *Квадратичный закон взаимности Гаусса.* $(\frac{q}{p})=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(\frac{p}{q})$.

Первообразные корни. Составители А. Канель и А. Скопенков.

1. (a) Если $(a,35)=1$, то $a^{12}\equiv 1\ (35)$.

(b) Если m делится на два различных простых нечетных числа и $(a,m)=1$, то $a^{\frac{\varphi(m)}{2}}\equiv 1\ (m)$.

Пусть $(g,m)=1$. Вычет g называется *первообразным корнем* по модулю m, если остатки от деления на m чисел $g^1,g^2,\dots,g^{\varphi(m)}\equiv 1$ различны.

2. (a) Если m делится на два различных простых нечетных числа, то не существует первообразного корня по модулю m.

(b) Пусть $x\equiv 1 \bmod 2$, x не сравнимо с 1 по модулю 4. Может ли $x^2\equiv 1 \bmod (2^{100})$?

(c)* При $n>2$ не существует первообразного корня по модулю 2^n.

3. (a) Число 2 является первообразным корнем по модулю 3^n. Указание: $2^2=1+3$.

(b) Число 2 является первообразным корнем по модулю 5^n. Указание: $2^4=1+5\cdot 3$.

(c) Найдите первообразный корень по модулю 7^n.

4. При каких n

(a) 2^n-1 делится на 3^{100}? (b) 2^n+1 делится на 3^{100}?

(c) 5^n-1 делится на 2^{100}? (d) 3^n+1 делится на 2^{100}?

5. Найти длину периода дроби (a) $1/3^{100}$; (b) $1/7^{100}$.

6. (a) При циклической перестановке цифр в периоде дроби $1/7=0,(142857)$ получатся дроби вида $1/7$, $2/7$, $3/7$, $4/7$, $5/7$, $6/7$. Докажите аналогичный факт для дроби $1/p$, если в ней длина периода равна $p-1$.

(b) Найдите множество остатков от деления чисел вида 10^k на 3^{100}.

(c) Докажите, что в разложении дроби $1/3^{100}$ встречается любая комбинация из 20 идущих подряд цифр.

7.* Найдите такие n, чтобы среди последних 1000 цифр числа 2^n нашлось 100 подряд идущих (a) нулей; (b) девяток.

8.* Аналогично задаче 7 вопрос про 5^n.

9. Положим $orda=ord_pa:=\min\{k\geq 1\mid a^k\equiv 1\ (p)\}$.

(a) Если $a^m \equiv a^n\ (p)$, то $m-n$ делится на $orda$. (b) $a \cdot ordx^a = ordx$.

(c) Если $ordx$ и $ordy$ взаимно просты, то $ord(xy) = ordx \cdot ordy$.

10. Если $p-1$ делится на d, то сравнение $x^d \equiv 1\ (p)$ имеет ровно d решений.

11. *Теорема о первообразном корне.* Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \ldots, g^{p-1} \equiv 1$ различны.

Докажите эту теорему для

(a) $p = 2^l + 1$; (b) $p = 2^k \cdot 3^l + 1$; (c) $p = 2^k \cdot 3^l \cdot 5^m + 1$; (d) общего случая.

$m/n = 1 + 1/2 + \ldots + 1/p$.

12. Если g первообразный корень по модулю простого $p > 2$, то

(a) существуют такие t и u, что $(g+pt)^{p-1} = 1 + pu$ и u не делится на p.

(b) Для любого целого положительного n существует первообразный корень по модулю p^n.

(c) То же по модулю $2p^n$.

13. Первообразные корни существуют только по модулям $2, 4, p^n, 2p^n$.

14. Пусть p — простое число, $x \equiv 1 \bmod (p^n)$, x не сравнимо с 1 по модулю p^{n+1}. Докажите, что:

(a) Если $(a,p) = 1$, то $x^a \equiv 1 \bmod p^n$, но x^a не сравнимо с 1 по модулю p^{n+1}.

(b) Докажите, что $x^p \equiv 1 \bmod p^{n+1}$, и если $n > 1$ либо $p > 2$, то x^p не сравнимо с 1 по модулю p^{n+2}.

24. Пусть $p > 2$ либо $n > 1$, $x \equiv 1 \bmod p^n$, x не сравнимо с 1 по модулю p^{n+1}, $a = p^k q$, q взаимно просто с p. Тогда $x^a \equiv 1 \bmod p^{n+k}$, x^a не сравнимо с p^{n+k+1}.