## Частные случаи

*Если из книги вытекает какой-нибудь поучительный вывод, он должен получаться помимо воли автора, в силу самих изображенных фактов.*

Ги де Мопассан

Из любых двух последовательных целых чисел $a$ и $a+1$ одно четное, а другое нечетное. Поэтому произведение $a(a+1)=a^2+a$ четно при любом целом $a$.

Делимость числа $a^2+a$ на 2 можно доказать и по-другому, разобрав два случая:

– если $a$ четно, то $a^2$ тоже четно, а сумма двух четных чисел $a$ и $a^2$ четна;

– если $a$ нечетно, то $a^2$ тоже нечетно, а сумма двух нечетных чисел $a$ и $a^2$ четна.

Вот так доказывают замечательное свойство многочлена $a^2+a$. Впрочем, при $\boldsymbol{p=2}$ в малой теореме Ферма фигурирует другой многочлен: $a^2-a=(a-1)a$. Все его значения в целых точках – четные числа (докажите!).

Теперь рассмотрим многочлен $\boldsymbol{a^3-a}$. Его легко разложить на множители:

$$a^3-a=a\left(a^2-1\right)=a(a-1)(a+1).$$

Получили произведение трех последовательных целых чисел: $a-1$, $a$ и $a+1$. Как мы уже знаем, это произведение четно. Поскольку из любых трех последовательных чисел одно кратно 3, их произведение $(a-1)a(a+1)=a^3-a$ кратно 3 (и, значит, даже кратно 6).

**Упражнение 1.** При любом целом $a$ сумма $a^3+5a$ кратна 6. Докажите это.

Многочлен $\boldsymbol{a^4-a}$ при $a=2$ и $a=3$ принимает значения $2^4-2=14$ и $3^4-3=78$. Конечно, эти значения четны, но никакого общего делителя кроме 2 (и 1) у них нет. Не повезло! Впрочем, число 4 составное, а малая теорема Ферма говорит только о многочленах вида $a^p-a$, где $p$ – простое число.

Пусть $\boldsymbol{p=5}$. Вычислим несколько значений многочлена $a^5-a$. При $a=\pm1$ и при $a=0$ получаем ноль. Смотрим дальше: $2^5-2=30$, $3^5-3=240$, $4^5-4=1020$, $5^5-5=3120$, $6^5-6=7770$,… Все эти значения кратны числу 30.

Поскольку $30=2\cdot3\cdot5$, доказательство делимости на 30 распадается на три части: во-первых, надо доказать, что $a^5-a$ кратно 2; во-вторых, $a^5-a$ кратно 3; в-третьих, $a^5-a$ кратно 5.

Первая часть очевидна: числа $a^5$ и $a$ либо оба четны, либо оба нечетны. Не вызывает затруднений и вторая часть:

$$a^5-a=a\left(a^4-1\right)=a\left(a^2-1\right)\left(a^2+1\right)=(a-1)a(a+1)\left(a^2+1\right),$$

произведение трех последовательных чисел всегда кратно 3.

Чуть сложнее третья часть. Нет, конечно, из пяти последовательных целых чисел обязательно одно кратно 5, так что произведение $(a-2)(a-1)a(a+1)(a+2)$ кратно 5. Но $a^2+1\neq(a-2)(a+2)$.

Как же быть? Самый бесхитростный способ – перебрать все подряд остатки от деления на 5: любое целое число при делении на 5 дает в остатке 0, 1, 2, 3 или 4. Если остаток равен 0, то кратен 5 второй множитель произведения $(a-1)a(a+1)(a^2+1)$. Если остаток равен 1 или 4, то кратен 5 первый или третий множитель. Если же остаток равен 2 или 3, то в дело вступает четвертый множитель. (Для тех, кто еще не привык работать с остатками, объясним: если $a=5b+2$, т. е. если $a$ дает остаток 2 при делении на 5, то $a^2+1=(5b+2)^2+1=5\left(5b^2+4b+1\right)$. Аналогично можно рассмотреть случай $a=5b+3$.)

Есть и другой способ:

$$a^2+1=(a-2)(a+2)+5,$$

значит, если нас интересуют только остатки от деления на 5, то $a^2+1$ можно-таки заменить на $(a-2)(a+2)$. Формулой это записывают так:

$$a^2+1\equiv(a-2)(a+2)\pmod 5.$$

Предложенное в 1801 году К. Ф. Гауссом обозначение «$\equiv$» еще не раз будет использовано нами. По определению, $a$ сравнимо с $b$ по модулю $n$, если $a-b$ кратно $n$, т. е. $a-b=kn$, где $k$ – целое число.

Обозначение

$$a\equiv b\pmod n$$

оказалось удачным потому, что свойства сравнений похожи на свойства обычных равенств. Сравнения можно складывать: если $a\equiv b\pmod n$ и $c\equiv d\pmod n$, то $a+c\equiv b+d\pmod n$. В самом деле, по определению, $a=b+kn$ и $c=d+ln$, где $k$, $l$ – целые числа. Значит,

$$a+c=(b+kn)+(d+ln)=b+d+(k+l)n,$$

что и требовалось.

Аналогично, формулы

$$a-c=(b+kn)-(d+ln)=b-d+(k-l)n,$$

$$ac=(b+kn)(d+ln)=bd+knd+bln+kln^2=$$
$$=bd+(kd+bl+kln)n$$

позволяют утверждать, что сравнения можно вычитать и умножать. Коли можно умножать, то можно и возводить в степень: если $a\equiv b\pmod n$, то для любого натурального числа $m$ верно сравнение $a^m\equiv b^m\pmod n$.

Сокращать сравнения надо с осторожностью:

$$6\equiv36\pmod{10},$$

но

$$1\not\equiv6\pmod{10}.$$

**Упражнения**

**2.** Решите сравнение $3x\equiv11\pmod{101}$.

**3.** Какие целые числа $x$ удовлетворяют сравнению $14x\equiv0\pmod{12}$?

**4.** Пусть $k\neq0$. Докажите, что а) если $ka\equiv kb\pmod{kn}$, то $a\equiv b\pmod n$;

б) если $ka\equiv kb\pmod n$ и числа $k$, $n$ взаимно просты, то $a\equiv b\pmod n$.

Продолжим изучение многочленов вида $a^p-a$: докажем, что при любом целом $a$ число $\boldsymbol{a^7-a}$ кратно 7. Как всегда, можно рассмотреть все 7 остатков от деления на 7: $0^7-0=0$, $1^7-1=0$, $2^7-2=126=7\cdot18$,…, $6^7-6=279930=7\cdot39990$. (Можно и чуточку сэкономить: поскольку любое целое число представимо в виде $a=7b$, $7b\pm1$, $7b\pm2$ или $7b\pm3$, очевидно, при проверке малой теоремы Ферма для $p=7$ можно ограничиться рассмотрением случаев $a=0$, 1, 2 и 3.)

Но бездумная проверка не может научить нас ничему интересному. Лучше рассмотрим разложение на