Гимназия 1543, математический спецкурс, 8 В

Занятие 15(д): квадратные сравнения

Решение квадратного уравнения

Напомним, как решаются квадратные уравнения в действительных (или комплексных) числах. Пусть мы имеем дело с уравнением
$$x^2 + ax + b = 0.$$
Путём очевидной замены $y = x + a/2$ мы приходим к эквивалентному уравнению вида
$$y^2 = c, \quad \text{где} \quad c = \frac{a^2}{4} - b.$$
По формуле разности квадратов $(y - \sqrt{c})(y + \sqrt{c}) = 0$, откуда $y = \pm\sqrt{c}$.

Применённая выше замена $y = x + a/2$ называется *выделением полного квадрата*. Она налагает единственное требование на арифметику, в которой решается уравнение: мы должны уметь делить на 2.

Квадратные сравнения по простому модулю

Данный листок посвящён квадратичным сравнениям в арифметике остатков. Мы не будем трогать составные модули, ограничившись лишь простыми.[1]

В арифметике по простому модулю p выделение полного квадрата возможно при любом $p > 2$. Если же $p = 2$, то $x^2 \equiv x$ и поэтому сравнение, на самом деле, не является квадратным. Поэтому мы будем считать, что $p > 2$, а полный квадрат уже выделен (т.е. мы имеем дело со сравнением вида $x^2 \equiv c \pmod{p}$).

Задачи

1) Докажите, что сравнение $x^2 \equiv c \pmod{p}$ имеет не более двух различных (по модулю p) решений.
2) Докажите, что сравнение $x^2 \equiv c \pmod{p}$ имеет единственное решение тогда и только тогда, когда $p \mid c$.
3) Докажите теорему Вильсона: число p простое тогда и только тогда, когда $(p-1)! \equiv -1 \pmod{p}$.

Определение. Пусть сравнение $x^2 \equiv c \pmod{p}$ имеет N различных решений. Число $(N-1)$ называется *символом Лежандра* и обозначается $\left(\dfrac{c}{p}\right)$.

4) Докажите, что $\left(\dfrac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. (Подсказка: казалось бы, причём здесь малая теорема Ферма?)
5) Докажите, что символы Лежандра обладают *мультипликативным* свойством:
$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$
6) Вычислите символы Лежандра $\left(\dfrac{0}{p}\right)$, $\left(\dfrac{1}{p}\right)$, $\left(\dfrac{4}{p}\right)$.
7) Вычислите символ Лежандра $\left(\dfrac{p-1}{p}\right)$.
8) Вычислите символ Лежандра $\left(\dfrac{2}{p}\right)$.
9) Докажите *квадратичный закон взаимности*: если для простых p, q, больших 2, верно $p \equiv q \equiv 3 \pmod{4}$, то $\left(\dfrac{q}{p}\right) = -\left(\dfrac{p}{q}\right)$, в противном случае $\left(\dfrac{q}{p}\right) = \left(\dfrac{p}{q}\right)$.
10) Вычислите $\left(\dfrac{257}{1543}\right)$.
11) Определите, разрешимо ли сравнение $x^2 + 631x \equiv 877 \pmod{1543}$.
12) Докажите, что если для простых p, q, больших 2, $p \equiv \pm q \pmod{4a}$, то $\left(\dfrac{a}{p}\right) = \left(\dfrac{a}{q}\right)$.

---

[1] Если модуль составной и представляет собой произведение различных простых чисел, то сравнение по такому модулю, согласно КТО, эквивалентно системе сравнений по модулям этих чисел. Если же модуль содержит какое-либо простое число в степени, большей 1, ситуация резко усложняется.