Экзамен «Элементы теории чисел»

Летняя многопрофильная школа при МЦНМО, кафедра математики, 2014

Экзамен засчитывается людям, сдавшим «Арифметика+» и умеющим решать следующие задачи:

1. Пусть $a, b \in \mathbb{N},\ d = (a, b)$. Докажите, что существуют такие $x, y \in \mathbb{Z}$, что $ax+by = d$. Более того, никакое натуральное число, меньшее d, не может быть представлено в виде линейной комбинации a и b.

2. Пусть bc делится на a, $(a, b) = 1$. Докажите, что c делится на a.

3. Докажите основную теорему арифметики. Любое натуральное число единственным образом разлагается в произведение простых чисел.

4. Покажите, что аналог основной теоремы арифметики не верен для множества натуральных чисел вида $4k + 1$.

5. Пусть $\varphi(n)$ — это количество натуральных чисел, не превосходящих n и взаимно простых с n. Вычислите $\varphi(1)$, $\varphi(6)$, $\varphi(27)$, $\varphi(1000000)$. Функция φ называется функцией Эйлера.

6. Докажите следующие свойства функции Эйлера, каждое из которых обобщает предыдущие:

1) если p — простое, то $\varphi(p) = p - 1$;
2) $\varphi(p^k) = p^k - p^{k-1}$;
3) $\varphi(m^k) = m^{k-1}\varphi(m)$

7. Пусть m и n взаимно просты. Докажите, что $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

8. Пусть $p_1, p_2, \ldots, p_k$ — все различные простые делители числа n. Докажите, что

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big) \cdot \ldots \cdot \Big(1 - \frac{1}{p_k}\Big).$$

9. Докажите теорему Эйлера:

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

10. Объясните общий принцип работы криптографических алгоритмов с открытым и ключем и детально опишите алгоритм RSA.