Vera Serganova

SOME PROBLEMS FROM NUMBER THEORY

1. *Pythagorean triples.* Three positive integers (x, y, z) form a Pythagorean triple if $x^2+y^2 = z^2$. The smallest and the most famous Pythagorean triple is (3,4,5). Show that any Pythagorean triple contains a number divisible by 3, a number divisible by 4 and a number divisible by 5.

2. Find all integers which can be represented as a difference of perfect squares, i.e. all $m = x^2 - y^2$.

3. Show that the equation $1 + x^2 + y^2 \equiv 0 \pmod p$ has a solution for any prime p.

4. Show that there are infinitely many prime numbers congruent to 3 modulo 4. The same is true for primes congruent to 1 modulo 4, but it is much harder to prove.

5. *Gaussian integers* are complex numbers with integral real and imaginary parts. A Gaussian integer z is prime if all its divisors are $\pm 1, \pm i, \pm z, \pm iz$. Note that 5 is not prime because $5 = (1 + 2i)(1 - 2i)$, but 7 is prime. Can you describe all Gaussian primes?

6. Fundamental theorem of arithmetics tells that an integer can be factored into a product of primes uniquely up to a change of signs of prime factors. Formulate and prove a similar statement for Gaussian integers. (Hint: define the Euclidean algorithm for Gaussian numbers).

7. Prove the Fermat formula

$$v(m) = 4 (d_1(m) - d_3(m)),$$

where $v(m)$ is the number of integral pairs (x, y) such that $m = x^2 + y^2$, $d_1(m)$ and $d_3(m)$ are the numbers of divisors of m congruent to 1 and 3 modulo 4 correspondingly.

8. Prove the Jacobi identity

$$\sum_{m=1}^{\infty} v(m) q^m = \sum_{n=0}^{\infty} (-1)^n \frac{q^{2n+1}}{1 - q^{2n+1}}.$$

Date: November 2, 2003.