**Занятие по арифметике №2. Группа Бронзы.**

*Многочлены по модулю. Квадратичные вычеты.*
*Польза сравнений. Varia.*

1. **Определение.** $\alpha$ – вычет по простому модулю $p$ – является корнем $mod\ p$ многочлена $f(x)$ с целыми коэффициентами, если $f(\alpha) \equiv 0 \pmod p$.

В этой задаче $p$ – простое число,все сравнения для многочленов $\mathrm{mod}p$ – формальные, то есть два многочлена сравнимы $mod\ p$, если сравнимы их коэффициенты при каждой степени $x$.

а) Докажите, что если $\alpha$ – корень многочлена $f(x) \bmod p$, то

$$f(x) \equiv (x-\alpha)g(x) \pmod p$$

для некоторого многочлена $g(x)$ с целыми коэффициентами.

б) Докажите, что если $\alpha_1, \alpha_2, \ldots, \alpha_k$ – корни многочлена $f(x)\ mod\ p$, то

$$f(x) \equiv (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)g(x)(modp)$$

для некоторого многочлена $g(x)$ с целыми коэффициентами.

в) Докажите, что многочлен степени $n > 0$ может иметь не более $n$ корней $\mathrm{mod}p$.

г) Докажите, что

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1)) \pmod p.$$

д) Выведите из утверждения п.г) теорему Вильсона.

2. $a$, $b$ и $n$ – фиксированные натуральные числа. Известно, что при любом натуральном $k$ $(k \neq b)$ число $a - k^n$ делится без остатка на число $b - k$. Докажите, что $a = b^n$.

3. а) 6, б) 15 простых чисел образуют арифметическую прогрессию. Докажите, что ее разность не меньше а) 30, б) 30000.

4. Докажите, что для каждого натурального $n$ существует бесконечно много $k$ таких, что $k \cdot 2^n - 7$ – точный квадрат.

5. Пусть $p > 2$ – простое число. Величину $D = b^2 - 4ac$ мы назовем *дискриминантом* сравнения $ax^2 + bx + c \equiv 0 \pmod p$. Докажите, что это сравнение

а) при $D \equiv 0 \pmod p$ имеет единственный корень (двойной);

б) при $\left(\frac{D}{p}\right) = 1$ имеет два различных корня, а при $\left(\frac{D}{p}\right) = -1$ не имеет корней.

6. Докажите, что для любого многочлена $x^2 + px + q$ с целыми коэффициентами существует такой многочлен $2x^2 + rx + s$ с целыми коэффициентами, что множества значений этих многочленов в целых точках не пересекаются.

7. Пусть $p = 8k + 1$ – простое число. Докажите, что:

а) $2 \cdot 4 \cdot 6 \cdot 8 \cdot \ldots \cdot 8k \equiv (-1)^{2k}(4k)! \pmod p$;

б) 2 – квадратичный вычет $\mathrm{mod}p$.

8. Решите в натуральных числах уравнение $3^n + 7 = k^2$.

9. $m$ и $n$ – натуральные числа, $m$ нечетно. Докажите, что $(2^m - 1, 2^n + 1) = 1$.

10. Найдите наибольшее целое число $x$ такое, чтобы число $4^{27} + 4^{1000} + 4^x$ являлось точным квадратом.

11. С натуральным числом, написанным на доске, разрешается проделать такую операцию: умножить его на выражение $(p-1)^2/p$, где $p$ – его простой делитель, и записать результат вместо исходного числа. Докажите, что, какое бы исходное число мы ни взяли и как бы мы ни проделывали описанные операции, на доске рано или поздно появится число 1.