theorem]Problem theorem]Solution

Midterm exam – MA1301–Tallteori
Wedndesday: October 9, 2013
Time: 10:15-12:00

Problem 1: Use the principle of mathematical induction to show that

$$\binom{2}{2} + \binom{3}{2} + \cdots \binom{n}{2} = \binom{n+1}{3}.$$

Solution: Basis step: $n = 1 : \binom{2}{2} = 1 = \binom{3}{3}$.

Induction step: We show that the statement

$$\binom{2}{2} + \binom{3}{2} + \cdots \binom{n}{2} = \binom{n+1}{3}.$$

implies the statement for $n+1$:

$$\binom{2}{2} + \binom{3}{2} + \cdots \binom{n}{2} + \binom{n+1}{2} = \binom{n+1}{3} + \binom{n+1}{2} = \binom{n+2}{3},$$

where we used the basic fact about binomial coefficients $\binom{n+1}{2} + \binom{n+1}{3} = \binom{n+2}{3}$.

Problem 2: Find the greatest common divisor of 326 and 78 and find integers x and y such that $\gcd(326, 78) = 326x + 78y$.

Solution: The Euclidean Algorithm allows one to compute the $\gcd(326, 78)$:

$$\begin{aligned} 326 &= 78 \cdot 4 + 14 \\ 78 &= 14 \cdot 5 + 8 \\ 14 &= 8 \cdot 1 + 6 \\ 8 &= 6 \cdot 1 + 2 \\ 6 &= 2 \cdot 3, \end{aligned}$$

thus $\gcd(326, 78) = 2$.

Now we find integers x and y such that $326x + 78y = 2$:

$$\begin{aligned} 2 &= 8 - 6 \\ &= 8 - 6 - (14 - 8) \\ &= 2 \cdot 8 - 14 \\ &= 2 \cdot (78 - 14 \cdot 5) - 14 \\ &= 2 \cdot 78 - 11 \cdot 14 \\ &= 2 \cdot 78 - 11 \cdot (326 - 78 \cdot 4) \\ &= 2 \cdot 78 - 11 \cdot 326. \end{aligned}$$

Therefore, we obtain that $2 \cdot 78 - 11 \cdot 326 = 2$, i.e. $x = 46$ and $y = -11$.

Problem 3: State the Chinese Remainder Theorem for three congruences and use it to solve the following system of congruences

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 5 \\ x &\equiv 3 \mod 7 \end{aligned}$$

Solution: Let n_1, n_2 and n_3 be integers with $\gcd(n_1, n_2) = \gcd(n_1, n_2) = \gcd(n_2, n_3) = 1$. Suppose a_1, a_2 and a_3 are integers. Then the simultaneous congruences

$$x \equiv a_1 \mod n_1 \text{ and } x \equiv a_2 \mod n_2 \text{ and } x \equiv a_3 \mod n_3$$

has exactly one solution x with $0 \leq x < n_1 n_2 n_3$.

Let us define the following numbers: $n = n_1 n_2 n_3$, $N_1 = n/n_1 = n_2 n_3$, $N_2 = n/n_2 = n_1 n_3$, $N_3 = n/n_3 = n_1 n_2$. Then $\gcd(N_k, n_k) = 1$ and $N_k x \equiv 1 \mod n_k$ has a solution x_k for $k = 1, 2, 3$. Then the integer

$$\overline{x} \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \mod n_1 \cdot n_2 \cdot n_3$$

is a solution to the three linear congruences.

Application to the case $n_1 = 3, n_2 = 5, n_3 = 7$ and $a_1 = 1, a_2 = 2, a_3 = 3$. Then

$$n = 105,\ n_1 = 35,\ n_2 = 21,\ n_3 = 7$$

and we have to find x_1, x_2, x_3 for

$$35x_1 \equiv 1 \mod 3,$$

$$21x_2 \equiv 1 \mod 5,$$

$$15x_3 \equiv 1 \mod 7,$$

which yields $x_1 = -1, x_2 = 1$ and $x_3 = 1$. Therefore, the solution is

$$\overline{x} \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 1 \cdot 35 \cdot (-1) + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 52 \equiv 105.$$

Problem 4: Compute $2^{32} \mod 37$ via repeated squaring and with the help of Fermat's Little Theorem. (For the second method use that $2^{36} = 2^4 2^{32}$.)

Solution: Repeated Squaring:

$$\begin{aligned} 2^2 &\equiv 4 \mod 37 \\ 2^4 &\equiv 16 \mod 37 \\ 2^8 &\equiv 256 \equiv 34 \mod 37 \\ 2^{16} &\equiv (-3)^2 \equiv 9 \mod 37 \\ 2^{32} &\equiv 81 \mod 37 \\ 2^{32} &\equiv 7 \mod 37 \end{aligned}$$

Computation via Fermat's Little Theorem: $2^3 6 \equiv 1 \mod 37$ implies that we have to compute $16x \equiv 1 \mod 37$, which amounts to solve

$$16x - 37y = 1.$$

Euclid's algorithm gives that $16 \cdot 7 - 3 \cdot 37 = 1$, i.e. $x = 7$.

$$2^{32} \cdot 16 \equiv 1 \mod 32$$

yields after multiplication by 7:

$$2^{32} \equiv 7 \mod 32.$$

Problem 5: Prove that $\sqrt{5}$ is an irrational number.

Solution: The proof is by contradiction: Suppose there exists integers a, b with $\gcd(a, b) = 1$ such that $a^2/b^2 = p$. Then $a^2 = pb^2$ and p divides a. By the prime divisor property: p divides a^2 and thus p divides a. Write $a = pA$, which yields $pA^2 = b^2$. By the same reasoning we obtain that p divides b, which is a contradicition to $\gcd(a, b) = 1$.