Solutions Number Theory Moed A 2014

D. Ginzburg

Problem 1: Prove that

$$\prod_{p|n}(1-p^{-2}) \le \frac{\sigma(n)\phi(n)}{n^2} \le 1 \tag{1}$$

Here, $\phi(n)$ is Euler's function, and $\sigma(n) = \sum_{d|n} d$.

Solution: Let $n = p_1^{u_1}\cdots p_r^{u_r}$ be the factorization of n into primes. In class we proved the following

$$\phi(n) = n\prod_{j=1}^{r}(1-p_j^{-1}) \qquad \sigma(n) = \prod_{j=1}^{r}\frac{p_j^{u_j+1}-1}{p_j-1} = n\prod_{j=1}^{r}\frac{1-p_j^{-u_j-1}}{1-p_j^{-1}}$$

where the right most equality is obtained by pulling out $p_j^{u_j+1}$ from the numerator, and p_j from the denominator.

Hence, we have

$$\frac{\sigma(n)\phi(n)}{n^2} = \prod_{j=1}^{r}(1-p_j^{-u_j-1})$$

From this, the right hand side inequality of equation (1) follows. Also, we have $u_j \ge 1$ for all $1 \le j \le r$, and hence $u_j+1 \ge 2$. Hence $p_j^{u_j+1} \ge p^2$, or $p^{-2} \ge p_j^{-u_j-1}$, and hence $(1-p_j^{-u_j-1}) \ge (1-p^{-2})$.

Problem 2: Find the smallest positive natural number n such that the equation $10x^2 - 12xy + 5y^2 = n$ has a solution in integers. For this value of n, solve the equation.

Solution: We first transfer $10x^2 - 12xy + 5y^2$ to a reduced form. Let $A_1 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ and $A_2 = \begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix}$. Then, applying the Theorem we proved in class, using A_1, the form $(10, -12, 5)$ is equivalent to $(5, 12, 10)$. Using A_2 on $(5, 12, 10)$ we get $(5, 2, 3)$, and finally using A_1 we get $(3, -2, 5)$. This is a reduced form. Thus, we look for the smallest n such that $3x^2 - 2xy + 5y^2 = n$. It is easy to see that $n = 3$, which is obtained by $(x, y) = (1, 0)$.

To find a solution to $10x^2 - 12xy + 5y^2 = 3$, we go backwards with the matrices A_i. Staring with the vector $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, we have $v_2 = A_1 v_1 = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$. Then, $v_3 = A_2 v_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, and finally, $v_4 = A_1 v_3 = \begin{pmatrix} -1 \\ -1 \end{pmatrix}$. So $(x, y) = (-1, -1)$ is the desired solution.

Problem 3: Let p be an odd prime greater than three. Assume that p divides $n^2 - n + 1$ for some positive integer n. Prove that $p \equiv 1 \pmod 3$.

Solution: If p divides $n^2 - n + 1$, then p divides $4(n^2 - n + 1) = 4n^2 - 4n + 4 = (2n-1)^2 + 3$. Hence we have $(2n-1)^2 \equiv -3 \pmod p$. Hence $\left(\frac{-3}{p}\right) = 1$. We have

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

Hence $p \equiv 1 \pmod 3$.

Problem 4: Let p be an odd prime. Solve the equation $6(p-3)! \equiv x \pmod p$.

Solution: By Wilson Theorem we have $(p-1)! \equiv -1 \pmod p$. Hence, multiplying the equation $6(p-3)! \equiv x \pmod p$ by $(p-2)(p-1)$ we obtain $6(p-1)! \equiv x(p-2)(p-1) \pmod p$, or, using Wilson's Theorem, $-6 \equiv x(p-2)(p-1) \pmod p$. But $(p-2)(p-1) \equiv 2 \pmod p$. Hence, we obtain $-3 \equiv x \pmod p$.