Math 100A: Homework 4

Merrick Qiu

Problem 1

By the Chinese Remainder Theorem, the statement is true for $n = 2$.

Let $r_1, r_2, \dots, r_k$ be pairwise coprime positive integers. Assume that the canonical map

$$\mathbb{Z}/(r_1 \cdots r_{k-1}\mathbb{Z}) \to (\mathbb{Z}/r_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/r_{k-1}\mathbb{Z})$$

is an isomorphism for $n = k - 1$. Since r_k is coprime with r_1 and r_2, we can write

$$ar_1 + br_k = 1$$

$$cr_2 + dr_k = 1$$

Multiplying these two equations yields

$$\begin{aligned}(ar_1 + br_k)(cr_2 + dr_k) &= acr_1r_2 + bcr_2r_k + adr_1r_k + bdr_k^2 \\ &= ac(r_1r_2) + (bcr_2 + adr_1 + bdr_k)r_k \\ &= 1\end{aligned}$$

Therefore r_k is coprime with r_1r_2. By induction, r_k is coprime with the product $r_1r_2 \dots r_{k-1}$. Applying the chinese remainder theorem on $r_1 \cdots r_{k-1}$ and r_k yields

$$\begin{aligned}\mathbb{Z}/((r_1 \cdots r_{k-1})r_k\mathbb{Z}) &\to \mathbb{Z}/(r_1 \cdots r_{k-1}\mathbb{Z}) \times (\mathbb{Z}/r_k\mathbb{Z}) \\ &\to ((\mathbb{Z}/r_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/r_{k-1}\mathbb{Z})) \times (\mathbb{Z}/r_k\mathbb{Z})\end{aligned}$$

Therefore

$$\mathbb{Z}/(r_1 \cdots r_k\mathbb{Z}) \to (\mathbb{Z}/r_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/r_k\mathbb{Z})$$

is an isomorphism, which by induction shows that the statement is true for all n.

Problem 2

When an element $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ is equal to its inverse, then $x^2 \equiv 1 \mod p$. This implies that

$$(x-1)(x+1) \equiv 0 \mod p$$

so x is equal to its inverse if and only if $x \equiv 1 \mod p$ or $x \equiv -1 \equiv p-1 \mod p$. This implies that $(p-2)! \equiv 1 \mod p$ since each element in the product $2 \cdot 3 \cdots p-2$ has a distinct inverse that is also in the product. Therefore

$$\begin{aligned}(p-1)! &\equiv (p-2)! \cdot (p-1) \\ &\equiv 1 \cdot (-1) \\ &\equiv -1 \mod p.\end{aligned}$$

Problem 3

x and y are equivalent to one of $0, 1, 2, 3 \mod 4$. Note that

$$\begin{aligned} 0^2 &\equiv 0 \mod 4 \\ 1^2 &\equiv 1 \mod 4 \\ 2^2 &\equiv 0 \mod 4 \\ 3^2 &\equiv 1 \mod 4. \end{aligned}$$

Thus the sum of the squares $x^2 + y^2$ can only be equal to $0, 1, 2 \mod 4$. Therefore there does not exist integers $x^2 + y^2 = n$ when $n \equiv 3 \mod 4$.

Problem 4

Since $p \equiv 1 \mod 4$, we can write $p = 4n + 1$ for some n. Therefore the multiplicative group modulo p has $4n$ elements.

Wilson's theorem says that the square of the product of the numbers 1 to $\frac{p-1}{2} = 2n$ is $-1 \mod p$.

$$\begin{aligned}
(p-1)! &\equiv 1 \cdot 2 \cdot \ldots \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdot \ldots \cdot (p-2) \cdot (p-1) \\
&\equiv 1 \cdot 2 \cdot \ldots \cdot \left(\frac{p-1}{2}\right) \cdot \left(1 - \frac{p+1}{2}\right) \cdot \ldots \cdot -2 \cdot -1 \\
&\equiv \Pi_{i=1}^{2n} i \cdot (-i) \\
&\equiv \Pi_{i=1}^{2n} i^2 \\
&\equiv -1 \mod p
\end{aligned}$$

Therefore we can choose $x =\equiv \Pi_{i=1}^{2n} i$ to satisfy the equation $x^2 + 1 \equiv 0 \mod p$.