2015-09-21 Problems

Introduction to Number Theory

Reference: "Number Theory 1: Fermat's dream" Kato, Kurokawa, Saito, Chapter 2.

1. Find some rational points on $x^2 + y^2 = 5$ other than $(\pm 1, \pm 2)$, $(\pm 2, \pm 1)$.

2. Let v be either a prime number or ∞. Let $a, b \in \mathbb{Q}^\times$. Prove the following statements:
2.1. $(a,b)_v = (b,a)_v$.
2.2. $(a,bc)_v = (a,b)_v(a,c)_v$.
2.3. $(a,-a)_v = 1$
2.4. $(a, 1-a)_v = 1$ if $a \neq 1$.
2.5. Let p be an odd prime. Let $a, b \in (\mathbb{Z}_{(p)})^\times$.
2.5.1. $(a,b)_p = 1$
2.5.2. $(a,pb)_p = \left(\dfrac{a \bmod p}{p}\right)$.
2.6. Let $a, b \in \mathbb{Z}_{(2)}^\times$.
2.6.1. $(a,b)_2 = 1$ if $a \equiv 1 \pmod 4$ or $b \equiv 1 \pmod 4$.
2.6.2. $(a,b)_2 = -1$ if $a \equiv b \equiv -1 \pmod 4$.
2.6.3.
$$(a,2b)_2 = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 8 \text{ or } a \equiv 1-2b \pmod 8. \\ -1 & \text{otherwise.} \end{cases}$$

3. In this exercise, we will prove the following theorem:
Theorem. Let $a, b \in \mathbb{Q}^\times$. Then $(a,b)_v = 1$ for almost all v and

$$\prod_v (a,b)_v = 1$$

where v runs over all the prime numbers and ∞.
Using the previous exercise and prime factorizations of a and b, we are reduced to the following three cases:
(i) a and b are distinct odd prime numbers,
(ii) a is an odd prime, and $b = -1$ or $b = 2$,
(iii) $a = -1$, and $b = -1$ or $b = 2$.
3.1. In Case (i), show

$$(a,b)_v = \begin{cases} \left(\frac{b}{a}\right) & \text{if } v = a, \\ \left(\frac{a}{b}\right) & \text{if } v = b, \\ (-1)^{\frac{a-1}{2}\frac{b-1}{2}} & \text{if } v = 2, \\ 1 & \text{otherwise.} \end{cases}$$

Now deduce the theorem in this case using the quadratic reciprocity law.

3.2.1. In Case (ii), show that

$$(a,-1)_v = \begin{cases} \left(\frac{-1}{a}\right) & \text{if } v = a, \\ (-1)^{\frac{a-1}{2}} & \text{if } v = 2, \\ 1 & \text{otherwise.} \end{cases}$$

3.2.2. In Case (ii), show that

$$(a,2)_v = \begin{cases} \left(\frac{2}{a}\right) & \text{if } v = a, \\ (-1)^{\frac{a^2-1}{8}} & \text{if } v = 2, \\ 1 & \text{otherwise.} \end{cases}$$

3.2.3. Deduce the theorem for Case (ii) from the (supplementary) quadratic reciprocity law.
3.3.1. Show

$$(-1,-1)_v = \begin{cases} -1 & \text{if } v = 2 \text{ or } \infty, \\ 1 & \text{otherwise.} \end{cases}$$

3.3.2. Show

$$(-1,2)_v = 1 \text{ for all } v.$$

3.3.3. Deduce the theorem for Case (iii) from the (supplementary) quadratic reciprocity law.

4. Show that $(1+2\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \times (1+4\mathbb{Z}_2)$. Here, $(1+4\mathbb{Z}_2) \subset (1+2\mathbb{Z}_2) \subset \mathbb{Q}_2^\times$ are groups under multiplication.

5. Let k be a field. Let $a, b, c \in k^\times$ and $r \in k$. Suppose $r^2 - a = bc$. Set

$$X = \{(x,y,z) \in k^3 \mid ax^2 + by^2 = z^2, (x,y,z) \neq (0,0,0)\},$$
$$Y = \{(x,y,z) \in k^3 \mid ax^2 + cy^2 = z^2, (x,y,z) \neq (0,0,0)\}.$$

Show that $X \cong Y$. Use that the following maps $f : X \to Y, g : Y \to X$ are inverses of one another:

$$f(x,y,z) = (rx + z, by, ax + rz),$$
$$g(x,y,z) = \left(\frac{rx - z}{r^2 - a}, \frac{y}{b}, \frac{-ax + rz}{r^2 - a}\right).$$

6. Let p be an odd prime. Show that $(1+p\mathbb{Z}_p)^2 = (1+p\mathbb{Z}_p)$. Is it true for $p = 2$?

7. Let $p \neq 2, 3$ be a prime number. Show that there exists a square root of -3 in $\mathbb{F}_p$ if and only if $p \equiv 1 (\mathrm{mod}\, 3)$.