33) Construction of the integers via an equivalence relation on $\mathbb{P}\times\mathbb{P}$. ($\mathbb{P}$ = positive integers)

The equivalence relation on $\mathbb{P}\times\mathbb{P}$:

Two pairs (a_1, b_1) and (a_2, b_2) in $\mathbb{P}\times\mathbb{P}$ are related, and we write $(a_1,b_1)\sim(a_2,b_2)$, if $a_1+b_2 = a_2+b_1$. (*)

Note: We think of $(a,b)\in\mathbb{P}\times\mathbb{P}$ as the integer $a-b$.

$\sim$ is reflexive: $(a,b)\sim(a,b)$, since $a+b=a+b$.

$\sim$ is symmetric: $(a_1,b_1)\sim(a_2,b) \Rightarrow (a_2,b_2)\sim(a_1,b_1)$.

Indeed,

$(a_1,b_1)\sim(a_2,b_2) \overset{def}{\Leftrightarrow} a_1+b_2=a_2+b_1$

$(a_2,b_2)\sim(a_1,b_1) \overset{def}{\Leftrightarrow} a_2+b_1=a_1+b_2$

and the right hand sides of the above two equivalences are equivalent, since equality is a symmetric relation on $\mathbb{P}$.

$\sim$ is transitive: we need to show:

$(a_1,b_1)\sim(a_2,b_2)$ and $(a_2,b_2)\sim(a_3,b_3) \Rightarrow (a_1,b_1)\sim(a_3,b_3)$.

The definition of $\sim$ translates the above to:

$a_1+b_2=a_2+b_1$ and $(a_2+b_3)=a_3+b_2) \Rightarrow (a_1+b_3)=(a_3+b_1)$.

Summing the left hand sides of the two equalities in the hypothesis of the above implication and equating to the sum of the right hand sides we get $a_1 + b_2 + a_2 + b_3 = a_2 + b_1 + a_3 + b_2$,

which implies $a_1 + b_3 = b_1 + a_3$.

Definition of the integers $\mathbb{Z}$:

Take $\mathbb{Z}$ to be the set of equivalence classes in $\mathbb{P} \times \mathbb{P}$ w.r.t the relation $\sim$.
Define addition by

$$[(a_1, b_1)] + [(a_2, b_2)] = [(a_1 + a_2, b_1 + b_2)].$$

[Remark: The above corresponds to the identity
$(a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$
in $\mathbb{Z}$.]

Proof that addition is well defined:

If $(a_1, b_1) \sim (c_1, d_1)$ and $(a_2, b_2) \sim (c_2, d_2)$
then $a_1 + d_1 = b_1 + c_1$ and $(a_2 + d_2) = b_2 + c_2$

So $a_1 + a_2 + d_1 + d_2 = b_1 + c_1 + b_2 + c_2$.
Hence $(a_1 + a_2, b_1 + b_2) \sim (c_1 + c_2, d_1 + d_2)$,

and addition is indeed well defined.

37)

a) If $k, m \in \mathbb{Z}$ and $\gcd(k,m)=1$, then $\gcd(k^2, m^2)=1$.

<u>Proof</u>: Let p be a prime, which is a common divisor of k^2 and m^2.

$p \mid k^2 \Rightarrow p \mid k$, by Thm 2.53.

$p \mid m^2 \Rightarrow p \mid m$, " " " .

Hence, p is a common divisor of k and m.

Now $\gcd(k,m)=1 \Leftrightarrow$

There does not exist a prime p, which is a common divisor of k and m.

$\Rightarrow$

There does not exist a prime p, which is a common divisor of k^2 and m^2

$\Rightarrow$

$\gcd(k^2, m^2)=1$.

b) If $x \in \mathbb{Q}$ and $x^2 \in \mathbb{Z}$, then $x \in \mathbb{Z}$.

<u>Proof</u>: Let p, q be two integers with $q>0$, such that $\gcd(p,q)=1$ and $x=\frac{p}{q}$.

Then $x^2 = \frac{p^2}{q^2}$, and $\gcd(p^2, q^2)=1$.

If $x^2 = a \in \mathbb{Z}$, then $x^2 = \frac{a}{1}$ and $\gcd(a,1)=1$.

The uniqueness of the above representation (Prop. 5.11) implies that $p^2=a$, $q^2=1$. Hence, $q=1$. So $x=p$ belongs to $\mathbb{Z}$.

37

c) If p is prime, then there does not exist a rational number whose square is p.

(By contradiction)

<u>Proof:</u> Let x be a rational number satisfying $x^2 = p$. Then x^2 is an integer, and so x is an integer as well, by part b. We may assume $x > 0$, since $x^2 = (-x)^2$. Since $p > 1$, then $x > 1$ as well (otherwise $x = 1$ and $x^2 = 1$). Furthermore, $p < p^2$, hence $x \neq p$. It follows that there exists a positive integer x, other than 1 and p, which divides $x^2 = p$. This contradicts the assumption that p is prime. Hence such x does not exist.

Q.E.D.