ELEMENTARY NUMBER THEORY

SOLUTIONS - LECTURE 1

Letters $a,b,c,\dots,m,n$ denote integers.

(1) The triple (a,b,c) is said to be a *pythagorean triple* if $a^2+b^2=c^2$. If (a,b,c) is a pythagorean triple, show that $60|abc$.

SOLUTION. Since $60=3\cdot4\cdot5$, it suffices to show that $3,4$ and 5 divide the product abc. Suppose 3 does not divide abc, then by Fermat's Theorem

$$a^2+b^2=1+1=2=1=c^2 \pmod 3,$$

which is impossible. Thus $3|abc$. Now, suppose 5 does not divide a and b, then $a^2=\pm1 \pmod 5$, $b^2=\pm1 \pmod 5$, and thus $a^2+b^2 \pmod 5$ is either $2,-2$ or 0. Since $c^2\not\equiv\pm2 \pmod 5$, necessarily $5|c$.

Finally, suppose 4 does not divide a and c, then

$$b^2=c^2-a^2=(c+a)(c-a).$$

Examining the possible cases we conclude that $8|b^2$, and thus $4|b$ (Why?). The remaining cases are trivial. ♦

(2) Show that

$$\sum_{k=1}^{n}\frac{1}{k}$$

cannot be an integer for $n>1$.

SOLUTION. Let 2^l be the greatest power of two in the set $\{1,2,\dots,n\}$, and 2^k the greatest power of two that divides $n!$. Clearly $l\le k$. Denote $n!\equiv2^k\gamma$, with γ not divisible by two. Then, if the sum equals a,

$$\frac{2^k\gamma}{1}+\frac{2^k\gamma}{2}+\cdots+\frac{2^k\gamma}{2^l}+\cdots+\frac{2^k\gamma}{n}=2^k\gamma a.$$

Date: December 22, 2015.

Since the exponent of two in the factorization of each $b(\neq 2^l) \in \{1,2,\dots,n\}$ is less that l (why?), dividing by 2^{k-l} above equation we lead to

$$\underbrace{\underbrace{\frac{2^l\gamma}{1}}_{\text{even}} + \underbrace{\frac{2^l\gamma}{2}}_{\text{even}} + \cdots + \underbrace{\gamma}_{\text{odd}} + \cdots + \underbrace{\frac{2^l\gamma}{n}}_{\text{even}}}_{\text{odd}} = \underbrace{2^{k-l}\gamma a}_{\text{even}},$$

what is impossible. ♦

(3) If $2^n - 1$ is prime, show that n is prime.

SOLUTION. Suppose $n = p \cdot m$, where p is a prime number. Then

$$2^{p\cdot m} - 1 = (2^p - 1)^m = 0 \pmod{2^p - 1},$$

contradiction. ♦

(4) If

$$\frac{1}{a} - \frac{1}{b} = \frac{1}{c}$$

and $h := (a,b,c)$, show that both $abch$ and $h(b-a)$ are perfect squares.

SOLUTION. WLOG $h = 1$ (why?). Then, since $(b-a) = ab/c$, we have that abc is a prefect square iff $b-a$ is a perfect square.

Now, let $d := (a,b)$, then $cd(a'-b') = d^2a'b'$, where $a' := a/d$ and $b' := b/d$. This leads to $d|c$, but a,b and c were relatively prime numbers, therefore $d = 1$.

Finally, $b = a+1$. Indeed, since $b-a|ab$, but

$$(ab, b-a) = (b^2, b-a) = 1,$$

so necessarily $b-a = 1$. Hence, $b-a = 1 = 1^2$. ♦

(5) If n is an even number, is possible to write 1 as the sum of the reciprocals of n odd numbers?

SOLUTION. No. Suppose

$$1 = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n},$$

where $a_1, a_2, \dots, a_n$ are odd numbers. Then

$$\underbrace{a_1a_2\dots a_n}_{\text{odd}} = \underbrace{(a_2a_3\dots a_n) + (a_1a_3\dots a_n) + \cdots + (a_1a_2\cdots a_{n-1})}_{\text{sum of an even number of odd numbers} \equiv \text{even}},$$

what is impossible. ♦

(6) Let p be a prime number. Given distinct integers m and n, there is an unique $t = t(m,n)$ such that $m - n = p^t k$ where k is an integer not divisible by p. Define a function $d\colon \mathbf{Z}\times\mathbf{Z} \to \mathbf{R}$ by the correspondence $d(m,n) = 0$ for $m = n$ and $d(m,n) = p^{-t}$ for $m \neq n$. Prove that $(\mathbf{Z}, d)$ is a metric space.

SOLUTION. The pair $(\mathbf{Z}, d)$ is a metric space as

(a) $d(m,n) \geq 0$.
(b) $d(m,n) = 0$ iff $m = n$, since $p^{-t} > 0$ for each t.
(c) $d(m,n) = d(n,m)$ for if $m - n = p^t \cdot k$, then $n - m = p^t \cdot (-k)$.
(d) Let

$$x - y = p^t \cdot k,$$
$$z - x = p^{t'} \cdot k'.$$

There are two possible cases to examine.

(i) If $t < t'$, then $z - y = p^t(k + p^{t'-t}k')$. Since $p \nmid (k + p^{t'-t}k')$, necessarily $t(y,z) = t$, and thus

$$d(x,y) = \frac{1}{p^t} \leq \frac{1}{p^{t'}} + \frac{1}{p^t} = d(x,y) + d(z,y).$$

(ii) If $t \geq t'$, then

$$d(x,y) = \frac{1}{p^t} \leq \frac{1}{p^{t'}} + \frac{1}{p^{t(y,z)}} = d(x,y) + d(z,y).$$

♦