Homework #1 Solutions — Math 3E fall 06-07

p.15 #1.5 Prove that $1^2+2^2+\dots+n^2 = \frac{1}{6}n(n+1)(2n+1)$
$= \frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n$

The second ~~inequality~~ equality comes by expanding the parentheses.
Prove the first equality by induction on n.

$n=1$. LHS $= 1^2 = 1$
RHS $= \frac{1}{6}\cdot 1\cdot(2)(3) = 1$.
Thus true for $n=1$.

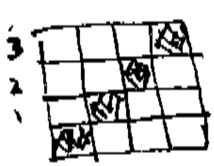
Induction hypothesis: assume true at stage n.

$n+1$: $1^2+2^2+\dots+n^2+(n+1)^2 = \frac{1}{6}n(n+1)(2n+1)+(n+1)^2$ by IH

$$= (n+1)\left[\frac{1}{6}n(2n+1)+(n+1)\right]$$
$$= (n+1)\left[\frac{1}{6}(n+2)(2n+3)\right]$$
$$= \frac{1}{6}(n+1)(n+2)(2(n+1)+1)$$

This verifies the identity at stage $n+1$.
Hence the result holds for all n by induction.

#1.11 Derive formula for $\sum_{i=1}^{n} i$ by computing the area $(n+1)^2$ of square with sides $n+1$.



It is clear by counting that the square of side length $n+1$ contains $(1+2+\dots+n)\times 2 + (n+1)$ small squares. Hence

$$\left(\sum_{i=1}^{n} i\right)\times 2 + (n+1) = (n+1)^2$$

or

$$\sum_{i=1}^{n} i = \frac{1}{2}(n+1)\,n \,.$$

<u>1.50</u> Prove that, if $d, d' \in \mathbb{Z}\setminus\{0\}$, $d \mid d'$ and $d' \mid d$ then $d = \pm d'$.

Since $d \mid d'$ there is $m \in \mathbb{Z}$ s.t. $d' = md$.

Since $d' \mid d$ there is $n \in \mathbb{Z}$ s.t. $d = nd'$.

Substituting gives $d' = m(nd') = mnd'$

Hence $mn = 1$. As m, n are integers, either $m = n = 1$ or $m = n = -1$.

Thus $d = d$ or $d = -d$.

<u>1.54</u> (i) Prove that, if n is square free then $\sqrt{n}$ is irrational.

(ii) Prove that $\sqrt[3]{2}$ is irrational.

(i) Suppose for contradiction that there is a rational number $\frac{a}{b}$ such that $\left(\frac{a}{b}\right)^2 = n$.

We may assume that a and b have no common factors. Let p be a prime which divides a. We have $a^2 = nb^2$, hence $p^2 \mid nb^2$.

By Corollary 1.40, as p^2 and b^2 are relatively prime, $p^2 \mid n$. This contradicts the assumption that n is square free.

(ii) Suppose for contradiction that $\left(\frac{a}{b}\right)^3 = 2$, where $\gcd(a,b) = 1$. Then $a^3 = 2b^3$, hence $2 \mid a^3$, and therefore $2 \mid a$. Thus $a = 2a'$, and hence $(2a')^3 = 2b^3$ i.e. $8a'^3 = 2b^3$, which implies $4a'^3 = b^3$. Thus $2 \mid b^3$, and ~~hence~~ $2 \mid b$. It follows that $\gcd(a,b) \geq 2$. $\times$

1.55(i) Find $d = \gcd(12327, 2409)$, write d as a linear combination of 12327 and 2409, and simplify the fraction $\frac{2409}{12327}$.

$b = 12327$, $a = 2409$

$12327 = 2409 \times 5 + 282$

$2409 = 282 \times 8 + 153$

$282 = 153 \times 1 + 129$

$153 = 129 \times 1 + 24$

$129 = 24 \times 5 + 9$

$$24 = 9 \times 2 + 6$$
$$9 = 6 \times 1 + 3$$
$$6 = 3 \times 2 + 0$$

Thus $\underline{\gcd(12327, 2409) = 3}$.

Now write each remainder as a linear combination of a, b.

$$282 = b - 5a.$$
$$153 = a - 8(282) = a - 8(b - 5a) = 41a - 8b.$$
$$129 = 282 - 153 = b - 5a - (41a - 8b)$$
$$= 9b - 46a.$$
$$24 = 153 - 129 = 41a - 8b - (9b - 46a)$$
$$= 87a - 17b$$
$$9 = 129 - 24 \times 5 = 9b - 46a - 5(87a - 17b)$$
$$= 94b - 481a$$
$$6 = 24 - 9 \times 2 = 87a - 17b - 2(94b - 481a) = 1049a - 205b$$
$$3 = 9 - 6 = 94b - 481a - (1049a - 205b)$$
$$\underline{3 = 299b - 1530a}$$

$$\frac{2409}{12327} = \frac{801}{4109} \text{ in lowest terms.}$$

$\underline{1.56}$ $a, b \in \mathbb{Z}$ s.t. $sa + tb = 1$ for some $s, t \in \mathbb{Z}$. Show that $\gcd(a, b) = 1$.

Suppose for contradiction that $\gcd(a, b) = d > 1$.
Then $a = md$, $b = nd$ for some $m, n \in \mathbb{Z}$.
So $smd + tnd = d(sm + tn) = 1$. This is impossible. $\blacksquare$

1.78 Use theorem 1.69 to solve congruence equations where possible. 5

(i) $3x \equiv 2 \mod 5$. Since $\gcd(3,5)=1$, solutions are $x \equiv s \times 2 \mod 5$, where $3s \equiv 1 \mod 5$. By inspection, $s=2$, thus all solutions are $\underline{x = 4+5k}$, $k \in \mathbb{N}$.

(ii) $7x \equiv 4 \mod 10$.

As above, solve $7s \equiv 1 \mod 10$

$$s = 3.$$

All solutions are $\underline{x = 2+10k}$, $k \in \mathbb{N}$.

(iii) $243x + 17 \equiv 101 \mod 725$

$$243x \equiv 84 \mod 725$$

Solve $243s \equiv 1 \mod 725$

Applying the euclidean algorithm gives $s = 182$.

Then solutions are $x = 84 \times 182 + 725k$

$$\underline{x = 63 + 725k, \ k \in \mathbb{N}}$$

(iv) $4x+3 \equiv 4 \mod 5$

$$4x \equiv 1 \mod 5$$

$$\underline{x = 4+5k, \ k \in \mathbb{N}}$$

(v) $6x+3 \equiv 4 \mod 10$

$6x \equiv 1 \mod 10$ – no solutions, as $(6,10)=2>1$.

(vi) $6x+3 \equiv 1 \mod 10$

$6x \equiv 8 \mod 10$ | $\underline{x = 3+10k, \ k \in \mathbb{N}}$

1.87 $x \in \mathbb{Z}$ satisfies $2 \nmid x$, $3 \nmid x$. Prove $x^2 \equiv 1 \mod 24$.

Write $x = 2n+1$. Then $x^2 = 4n^2 + 4n + 1$, so $x^2 \equiv 1 \mod 4$.

In fact, $x^2 = 4n(n+1) + 1$, and either $2 \mid n$ or $2 \mid (n+1)$,

so $x^2 \equiv 1 \mod 8$.

Thus $x^2 \equiv 1, 9,$ or $17 \mod 24$.

Write $x = 3m + a$, where $a = 1$ or 2. Then

$x^2 = 9m^2 + 6m + a^2$, so $x^2 \equiv 1 \mod 3$.

Of the above choices, only $x^2 \equiv 1 \mod 24$

satisfies the further requirement.

1.88 p is prime, $a^2 \equiv 1 \mod p$. Show that $a \equiv \pm 1 \mod p$.

Since $a^2 \equiv 1 \mod p$, $a^2 - 1 \equiv 0 \mod p$, i.e.

$p \mid (a^2 - 1)$; equivalently $p \mid (a-1)(a+1)$.

By Theorem 1.38, $p \mid (a-1)$ or $p \mid (a+1)$; that is,

$a \equiv 1 \mod p$ or $a \equiv -1 \mod p$.

Challenge Problems for Homework 1

1.23 Double induction: Given statements $S(m,n)$ satisfying

(i) $S(0,0)$ is true;

(ii) $S(m,0)$ true $\Rightarrow S(m+1,0)$ true;

(iii) if $S(m,n)$ is true for all $m \geq 0$ then $S(m,n+1)$ is true for all $m \geq 0$.

Prove that $S(m,n)$ is true for all $m \geq 0$, $n \geq 0$.

Let $P(n)$ be the statement "$\forall m \geq 0$ $S(m,n)$ holds".
We show, by induction on n, that $P(n)$ is true for all n. This is the required result.

$n=0$. We need to show $\forall m \geq 0$ $S(m,0)$ holds.
This is proved by induction on m, and (i), (ii) are the induction statements.

IH Assume $P(n)$ holds; $\forall m \geq 0$ $S(m,n)$ holds.

$n+1$ Need to show $\forall m \geq 0$ $S(m,n+1)$ holds.
This is exactly (iii).

Hence $P(n)$ holds for all n, as required.

1.67 Pythagorean triples.

(i) Let $z = q+ip$, $q,p \in \mathbb{N}$, $q > p$. Show that $(q^2-p^2, 2qp, q^2+p^2)$ is a Pythagorean triple.

(ii) Show that $(9,12,15)$ is not of the type in (i).

/8

(iii) Show that (19597501, 28397460, 34503301) is a Pythagorean triple by finding p, q.

(i) Note that, for any complex numbers z, w,
$|zw| = |z||w|$. Hence $|z^2| = |z||z| = |z|^2$.

Now, $|z|^2 = |q+ip|^2 = (q^2+p^2)^2$.

$|z^2| = |(q+ip)^2| = |q^2 - p^2 + i2qp|$
$= (q^2-p^2)^2 + (2qp)^2$.

Hence $(q^2-p^2, 2qp, q^2+p^2)$ is a Pythagorean triple.

(ii) Suppose there are integers q, p such that
$q^2-p^2 = 9, \quad 2qp = 12, \quad q^2+p^2 = 15$.
Subtracting gives $2p^2 = 15-9 = 6$ or $p^2 = 3$.
But $\sqrt{3}$ is not an integer, so there is no solution.

(iii) Solve $q^2-p^2 = 19597501$
$2qp = 28397460$
$q^2+p^2 = 34503301$

Subtracting gives $2p^2 = 14905800$ (note this does not need the calculator!)
$p^2 = 7452900$
$\underline{p = 2730}$

Substituting: $q = \frac{14198730}{2730} = \underline{5201}$

1.82 (i) Prove $7 \mid (10q+r)$ iff $7 \mid (q-2r)$.

(ii) Write $a = d_k 10^k + d_{k-1} 10^{k-1} + \dots + d_0 10^0$.

Define $a^{(1)} = d_k 10^{k-1} + d_{k-1} 10^{k-2} + \dots + d_1 10^0 - 2d_0$,

$a^{(2)} = d_k 10^{k-2} + d_{k-1} 10^{k-3} + \dots + d_2 10^0 - 2d_1$ etc.

Prove $7 \mid a \iff 7 \mid a^{(i)}$ for some $i = 1, \dots, k$.

(i) Suppose $7 \mid (10q+r)$. Then $10q + r = 7n$, so

$q - 2r = q - 2(7n - 10q) = 21q - 14n$, which is divisible by 7.

Conversely, suppose $7 \mid (q-2r)$. Then $q - 2r = 7m$, so

$10q + r = 10(7m + 2r) + r = 70m + 21r$, which is divisible by 7.

(ii) Suppose $7 \mid a$. Write $a = 10(d_k 10^{k-1} + \dots + d_1 10^0) + d_0$

$= 10q + r$.

Then by (i), $7 \mid (q - 2r)$, and $q - 2r = a^{(1)}$.

Conversely, suppose $7 \mid a^{(i)}$ for some $1 \le i \le k$.

Write $a^{(i)} = d_k 10^{k-i} + d_{k-1} 10^{k-i-1} + \dots + d_i 10^0 - 2d_{i-1}$

$= q - 2r$.

By (i), $7 \mid (10q + r)$ i.e. $7 \mid a^{(i-1)}$. By an obvious induction, it follows that $7 \mid a$.