PROBLEM SET 1
MATH 115
NUMBER THEORY
PROFESSOR PAUL VOJTA

NOAH RUDERMAN

Problems 1.2.1c, 1.2.2, 1.2.3e, 1.2.14, 1.2.19, 1.2.21, 1.3.6, 1.3.14, 1.3.16, 1.3.18, 1.3.21, 1.4.2, 1.4.6, and 1.4.9 from *An Introduction to The Theory of Numbers*, 5th edition, by Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery

Problem (1.2.1)

Solution.

c.

$$\begin{aligned}
\underbrace{3997}_{r_0} &= 1 * \underbrace{2947}_{r_1} + \underbrace{1050}_{r_2} \\
\underbrace{2947}_{r_1} &= 2 * \underbrace{1050}_{r_2} + \underbrace{847}_{r_3} \\
\underbrace{1050}_{r_2} &= 1 * \underbrace{847}_{r_3} + \underbrace{203}_{r_4} \\
\underbrace{847}_{r_3} &= 4 * \underbrace{203}_{r_4} + \underbrace{35}_{r_5} \\
\underbrace{203}_{r_4} &= 5 * \underbrace{35}_{r_5} + \underbrace{28}_{r_6} \\
\underbrace{35}_{r_5} &= 1 * \underbrace{28}_{r_6} + \underbrace{7}_{r_7} \\
\underbrace{28}_{r_6} &= 4 * \underbrace{7}_{r_7} + \underbrace{0}_{r_8}
\end{aligned}$$

$$\begin{aligned}
\gcd(2947, 3997) &= (r_7, r_8) \\
&= (7, 0) \\
&= 7
\end{aligned}$$

Date: June 30, 2014.

Problem (1.2.2)

Solution.

$$\begin{aligned}
\underbrace{3587}_{r_0} &= 1 * \underbrace{1819}_{r_1} + \underbrace{1768}_{r_2} \\
\underbrace{1819}_{r_1} &= 1 * \underbrace{1768}_{r_2} + \underbrace{51}_{r_3} \\
\underbrace{1768}_{r_2} &= 34 * \underbrace{51}_{r_3} + \underbrace{34}_{r_4} \\
\underbrace{51}_{r_3} &= 1 * \underbrace{34}_{r_4} + \underbrace{17}_{r_5} \\
\underbrace{34}_{r_4} &= 2 * \underbrace{17}_{r_5} + \underbrace{0}_{r_6}
\end{aligned}$$

So $\gcd(3587, 1819) = \gcd(r_5, r_6) = \gcd(17, 0) = 17$.

Next, $2 * 1819 - 1 * 3587 = 51$. Note that $3587 = 70 * 51 + 17$.

$$\begin{aligned}
3587 &= 70 * 51 + 17 \\
3587 &= 70 * (2 * 1819 - 3587) + 17 \\
-140 * 1819 + 71 * 3587 &= 17 \\
-140 * 1819 + 71 * 3587 &= \gcd(3587, 1819)
\end{aligned}$$

so $x = -140$, $y = 71$.

Problem (1.2.3)

Solution.

e. From
$$f(x,y,z) = 6x + 10y + 15z = 1,$$
we see that
$$f(x,y,z) \equiv 1 \mod n, n \in \mathbb{Z}^+.$$
For $n = 2, 3, 5$ we get the congruences
$$\begin{aligned} z &\equiv 1 \mod 2 \\ y &\equiv 1 \mod 3 \\ x &\equiv 1 \mod 5. \end{aligned}$$
The gcd of 6 and 10 is 2 such that $6 \cdot -3 + 10 \cdot 2 = 2$. Next, we see that
$$\begin{aligned} 6x + 10y &= 1 - 15z \\ &= 1 - 15(2k+1) \qquad \text{(since } z \text{ is odd)} \\ &= 1 - 30k - 15 \\ &= -14 - 30k \\ &= 2(-7 - 15k) \\ &= (6 \cdot -3 + 10 \cdot 2)(-7 - 15k) \\ &= 6 \cdot (3(7 + 15k)) + 10 \cdot (2(-7 - 15k)), \end{aligned}$$
so
$$\begin{aligned} z &= 2k + 1 \\ x &= 21 + 45k \\ y &= -14 - 30k \end{aligned}$$

Problem (1.3.14)

Solution.

If n is odd, we can write $n = 2k + 1$ for some $k \in \mathbb{Z}$. We have

$$\begin{aligned} n^2 - 1 &= (2k + 1)^2 - 1 \\ &= (4k^2 + 4k + 1) - 1 \\ &= 4k^2 + 4k \\ &= 4k(k + 1). \end{aligned}$$

Either k or $k + 1$ is even, so we can factor our 2 from one of these terms to get

$$4k(k + 1) = 8c,$$

for some $c \in \mathbb{Z}$. Since $8c = n^2 - 1$, $n^2 - 1$ is divisible by 8 by definition.

Problem (1.3.19)

Solution.

Suppose we have n distinct integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Given that

$$\gcd(a_i, a_j) = 1 \tag{1}$$

for $i \neq j$, if we consider the prime factorizationa

$$a_k = \prod_p p^{\alpha_k(p)}, 1 \leq k \in \mathbb{N} \leq n,$$

Then $\min(\alpha_i(p), \alpha_j(p)) = 0$ for all prime p. We prove that the set of numbers is relatively prime by contradiction. Suppose, they are not relatively prime. Then

$$\gcd(a_1, a_2, \ldots, a_n) \neq 1.$$

This implies that

$$\min(\alpha_1(p), \alpha_2(p), \ldots, \alpha_n(p)) \neq 0$$

for some prime p. From this we have,

$$\alpha_k(p) \geq 1$$

for all $1 \leq k \leq n$ for some p. Therefore

$$\min(\alpha_i(p), \alpha_j(p)) \geq 1 \tag{2}$$

for all i, j given some prime p. This contradicts equation 1. Therefore,

$$\gcd(a_1, a_2, \ldots, a_n) = 1$$

Problem (1.3.21)

Solution.

Regardless of the value of k, it is easy to see that $6k+5 \equiv 1 \mod 2$. Thus, we can write odd numbers of the form $6k+5$. If we can also write that number in the form $3k'-1$, then

$$\begin{aligned} 3k'-1 &\equiv 1 \mod 2 \\ 3k' &\equiv 2 \mod 2 \\ 3k' &\equiv 0 \mod 2 \\ k' &\equiv 0 \mod 2, \end{aligned}$$

so k' is even. Now we try to find a formula for k in terms of k' if a number can be written in both forms. We have

$$\begin{aligned} 6k+5 &= 3k'-1 \\ 6k-3k' &= -6 \\ 3(2k-k') &= -6 \\ 2k-k' &= -2 \\ k &= \frac{k'-2}{2}. \end{aligned}$$

Since k' is even, the term on the right is an integer. Thus, if a number can be written in the form $6k+5$, we can substitute $k = \frac{k'-2}{2}$ to recover the form $3k'-1$.

Problem (1.3.6)

Solution.

By the fundamental theorem of arithmetic, any number $n \in \mathbb{Z}^+$ can be written uniquely (up to a permutation) in form

$$n = \prod_p p^{\alpha(p)}$$

where p is prime. We can factor our factors of 2 to get

$$n = \underbrace{2^{\alpha(2)}}_{2^r} \underbrace{\prod_{p \neq 2} p^{\alpha(p)}}_{m}.$$

Since all primes other than 2 are odd, m is the product of odd numbers and must also be odd. Since $r = \alpha(2)$ and $\alpha(p) \geq 0$ for all prime p, $r \geq 0$, completing the proof.

Problem (1.3.14)

Solution.

In this proof I use the fact that if $\gcd(a, b) = d$ and $\gcd(a, c) = 1$ then $\gcd(a, bc) = d$. I also use the notation $p^e \parallel a$ for a prime p and $e, a \in \mathbb{Z}$ to mean that e is the highest power of p that divides a.

It is clear that from $\gcd(a, p^2) = p$ that $p \parallel a$. Thus, $np = a$ for some $n \in \mathbb{Z}$ where $\gcd(n, p) = 1$.

Likewise, from $\gcd(b, p^3) = p^2$ we see that $p^2 \parallel b$. Thus, $mp^2 = b$ for some $m \in \mathbb{Z}$ where $\gcd(m, p^2) = 1$. This also implies $\gcd(m, p) = 1$.

Now we can prove $\gcd(ab, p^4) = p^3$. We know that

$$\gcd(p^4, p^3) = p^3. \tag{3}$$

Since $\gcd(p, n) = 1$ and $\gcd(p, m) = 1$, $\gcd(p, nm) = 1$ and therefore

$$\gcd(p^4, nm) = 1. \tag{4}$$

Combining equations 3 and 4 we get

$$\begin{aligned} \gcd(p^4, mnp^3) &= 1 \\ \gcd(p^4, ab) &= 1 \\ \gcd(ab, p^4) &= 1 \end{aligned}$$

Now we aim to prove that $\gcd(a + b, p^4) = p$. We start with $\gcd(n + mp, p)$. Clearly this gcd is equal to 1 or p. If the gcd is p, then $p \mid n + mp$. Since $p \mid mp$, then $p \mid n$. But $\gcd(n, p) = 1$, so $p \not| n$. Thus, the gcd is 1 so

$$\gcd(p^4, n + mp) = 1 \tag{5}$$

Clearly,

$$\gcd(p^4, p) = p \tag{6}$$

Combining equations 5 and 6, we have

$$\begin{aligned} \gcd(p^4, p(n + mp)) &= p \\ \gcd(p^4, pn + mp^2) &= p \\ \gcd(p^4, a + b) &= p \\ \gcd(a + b, p^4) &= p \end{aligned}$$

Problem (1.3.16)

Solution.

From the description of n, we see that

$$n = 2a^2 = 3b^3 = 5c^5,$$

for some $a, b, c \in \mathbb{Z}^+$. Consider the prime factorization of n,

$$n = \prod_p p^{\alpha(p)} a$$

for primes p. We see that

$$\begin{aligned} \alpha(2) &\equiv 1 \mod 2 \\ \alpha(2) &\equiv 0 \mod 3 \\ \alpha(2) &\equiv 0 \mod 5 \end{aligned}$$

The solution is $\alpha(2) \equiv 15 \mod 30$.

Likewise,

$$\begin{aligned} \alpha(3) &\equiv 0 \mod 2 \\ \alpha(3) &\equiv 1 \mod 3 \\ \alpha(3) &\equiv 0 \mod 5 \end{aligned}$$

The solution is $\alpha(3) \equiv 10 \mod 30$.

Finally,

$$\begin{aligned} \alpha(5) &\equiv 0 \mod 2 \\ \alpha(5) &\equiv 0 \mod 3 \\ \alpha(5) &\equiv 1 \mod 5 \end{aligned}$$

The solution is $\alpha(5) \equiv 6 \mod 30$.

By guess and check, the factorization

$$n = 2^{15} \cdot 3^{10} \cdot 5^6$$

is a solution.

Problem (1.3.18)

Solution.

We aim to prove that $\gcd(a^2,b^2)=c^2 \iff \gcd(a,b)=c$. Let

$$a=\prod_p p^{\alpha(p)}$$

$$b=\prod_p p^{\beta(p)}$$

$(\longleftarrow)$
We see that

$$c=\prod_p p^{\min(\alpha(p),\beta(p))}$$

Clearly,

$$\begin{aligned} a^2 &= \left(\prod_p p^{\alpha(p)}\right)^2 \\ &= \prod_p \left(p^{\alpha(p)}\right)^2 \\ &= \prod_p p^{2\alpha(p)}, \end{aligned}$$

and

$$\begin{aligned} b^2 &= \left(\prod_p p^{\beta(p)}\right)^2 \\ &= \prod_p \left(p^{\beta(p)}\right)^2 \\ &= \prod_p p^{2\beta(p)}. \end{aligned}$$

Let $c'=\gcd(a^2,b^2)$. Then

$$c'=\prod_p p^{\min(2\alpha(p),2\beta(p))}.$$

But

$$\begin{aligned} c^2 &= \left(\prod_p p^{\min(\alpha(p),\beta(p))}\right)^2 \\ &= \prod_p \left(p^{\min(\alpha(p),\beta(p))}\right)^2 \\ &= \prod_p p^{2\cdot\min(\alpha(p),\beta(p))} \end{aligned}$$

$$= \prod_p p^{\min(2\alpha(p), 2\beta(p))}.$$

so $c^2 = c'$ and $\gcd(a, b) = c$ implies $\gcd(a^2, b^2) = c^2$.

$(\longrightarrow)$
To prove the converse, assuming $\gcd(a^2, b^2) = c^2$, we simply reverse the steps for how we calculated a^2, b^2 and c^2 to get formulas for a, b, c. We know that $\gcd(a, b) = \prod_p p^{\min(\alpha(p), \beta(p))}$, which is equal to c, so $c = \gcd(a, b)$.

Problem (1.3.21)

Solution.

We aim to prove that

$$\operatorname{lcm}(a, b, c) \cdot \gcd(ab, bc, ca) = |abc| . \tag{7}$$

Consider the prime factorization of both sides of the equation. They must be equal if each exponent for every prime in their prime factorization is equal. Let

$$a = \prod_p p^{\alpha(p)},$$

$$b = \prod_p p^{\beta(p)},$$

$$c = \prod_p p^{\gamma(p)}.$$

Consider an arbitrary prime p. The exponent for this prime on the left hand side is

$$\max(\alpha(p), \beta(p), \gamma(p)) + \min(\alpha(p) + \beta(p), \beta(p) + \gamma(p), \gamma(p) + \alpha(p)).$$

Suppose that $\alpha(p) \geq \beta(p) \geq \gamma(p))$. Then

$$\max(\alpha(p), \beta(p), \gamma(p)) = \alpha(p),$$

and

$$\min(\alpha(p) + \beta(p), \beta(p) + \gamma(p), \gamma(p) + \alpha(p)) = \beta(p) + \gamma(p),$$

so

$$\max(\alpha(p), \beta(p), \gamma(p)) + \min(\alpha(p) + \beta(p), \beta(p) + \gamma(p), \gamma(p) + \alpha(p)) = \alpha(p) + \beta(p) + \gamma(p).$$

We see that the right hand side is the exponent for the same prime in the prime factorization of $|abc|$.

Since the ordering of the exponents $\alpha(p), \beta(p)$ and $\gamma(p)$ was arbitrary, this holds for any ordering. Furthermore, since p was an arbitrary prime, this condition holds for any prime p. Thus the exponents for each prime are the same on each side of equation 7 so the equation is true.

Problem (1.4.2)

Solution.

We aim to show that for $n \in \mathbb{N} \geq 1$, that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0. \tag{8}$$

We show this with induction. Assume equation 8. We have

$$\begin{aligned}
\sum_{k=0}^{n+1} (-1)^k \binom{n+1}{k} &= \left[\sum_{k=0}^{n} (-1)^k \binom{n+1}{k}\right] + (-1)^{n+1} \binom{n+1}{k+1} \\
&= \left[\sum_{k=0}^{n} (-1)^k \left(\binom{n}{k} + \binom{n}{k-1}\right)\right] + (-1)^{n+1} \\
&= \underbrace{\sum_{k=0}^{n} (-1)^k \binom{n}{k}}_{=0 \text{ (by supposition)}} + \sum_{k=0}^{n} (-1)^k \binom{n}{k-1} + (-1)^{n+1} \\
&= \sum_{k=1}^{n} (-1)^k \binom{n}{k-1} + (-1)^{n+1} \\
&= \sum_{k=0}^{n-1} (-1)^{k+1} \binom{n}{k} + (-1)^{n+1} \\
&= \underbrace{\sum_{k=0}^{n} (-1)^{k+1} \binom{n}{k}}_{=0 \text{ by (*)}} - (-1)^{n+1} \binom{n}{n} + (-1)^{n+1} \\
&= -(-1)^{n+1} + (-1)^{n+1} \\
&= 0.
\end{aligned}$$

Here, (*) is from multiplying both sides of equation 8 by -1. Thus, the inductive step is true.

Next, we use the base case of $n = 1$, where

$$\begin{aligned}
\sum_{k=0}^{1} (-1)^k \binom{1}{k} &= (-1)^0 \binom{1}{0} + (-1)^1 \binom{1}{1} \\
&= 1 - 1 \\
&= 0,
\end{aligned}$$

completing the proof.

Problem (1.4.6)

Solution.

We aim to show that if $f(x), g(x)$ are n-times differentiable, then the n^{th} derivative of $f(x)g(x)$ is

$$\sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x). \tag{9}$$

We will prove this with induction. First, assume equation 9. Next,

$$\begin{aligned}
\frac{d}{dx} \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x) &= \sum_{k=0}^{n} \binom{n}{k} \left(f^{(k+1)}(x) g^{(n-k)}(x) + f^{(k)}(x) g^{(n+1-k)}(x) \right) \\
&= \sum_{k=0}^{n} f^{(k)}(x) g^{(n+1-k)}(x) \left(\binom{n}{k-1} + \binom{n}{k} \right) + f^{(n+1)}(x) g^{(0)}(x) \\
&= \sum_{k=0}^{n} f^{(k)}(x) g^{(n+1-k)}(x) \binom{n+1}{k} + f^{(n+1)}(x) g^{(0)}(x) \\
&= \sum_{k=0}^{n+1} f^{(k)}(x) g^{(n+1-k)}(x) \binom{n+1}{k}.
\end{aligned}$$

As our base case, suppose $n = 0$.

$$\begin{aligned}
\sum_{k=0}^{0} \binom{0}{k} f^{(k)}(x) g^{(0-k)}(x) &= \binom{0}{0} f^{(0)}(x) g^{(0)}(x) \\
&= f(x) g(x).
\end{aligned}$$

Thus, equation 9 is true for all $n \geq 0$.

Problem (1.4.9)

Solution.

We aim to prove this by induction. For our induction step, suppose that

$$\Delta^n f(x) = \sum_{j=0}^{k} (-1)^j \binom{k}{j} f(x+k-j) \tag{10}$$

We see that

$$\begin{aligned}
\Delta^{n+1} f(x) &= \Delta(\Delta^n f(x)) \\
&= \Delta \sum_{j=0}^{k} (-1)^j \binom{k}{j} f(x+k-j) \\
&= \sum_{j=0}^{k} (-1)^j \binom{k}{j} \Delta f(x+k-j) \\
&= \sum_{j=0}^{k} (-1)^j \binom{k}{j} \left(f(x+(k+1)-j) - f(x+k-j)\right) \\
&= \sum_{j=0}^{k} f(x+(k+1)-j) \left((-1)^j \binom{k}{j} - (-1)^{j-1} \binom{k}{j-1}\right) - f(x)(-1)^k \\
&= \sum_{j=0}^{k} f(x+(k+1)-j)(-1)^j \binom{k+1}{j} - f(x)(-1)^k \\
&= \sum_{j=0}^{k} f(x+(k+1)-j)(-1)^j \binom{k+1}{j} + f(x)(-1)^{k+1} \\
&= \sum_{j=0}^{k+1} (-1)^j \binom{k+1}{j} f(x+(k+1)-j),
\end{aligned}$$

completing the induction step.

As our base case, consider $k = 1$.

$$\begin{aligned}
\sum_{j=0}^{1} (-1)^j \binom{1}{j} f(x+1-j) &= (-1)^0 \binom{1}{0} f(x+1-0) + (-1)^1 \binom{1}{1} f(x+1-1) \\
&= f(x+1) + -f(x) \\
&= \Delta f(x)
\end{aligned}$$

by definition. Thus, equation is true for all $k \geq 1$.