PROBLEM SET 6
MATH 115
NUMBER THEORY
PROFESSOR PAUL VOJTA

NOAH RUDERMAN

Problems 3.7.1, 3.7.2, 3.7.3, 3.7.5, 4.1.2, 4.1.4, 4.1.6, 4.1.9, 4.2.2, 4.2.5, 4.2.6, 4.2.12, 4.2.16, 4.3.1, and 4.3.5 from *An Introduction to The Theory of Numbers*, 5^{th} edition, by Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery

Date: August 4, 2014.

Problem (3.7.1)

Let $f(x,y) = ax^2+bxy+cy^2$ be a reduced positive definite form. Show that all representations of a by f are proper.

Solution.

By theorem 3.24, a is the smallest number we can properly represent by f. For the sake of contradiction, suppose that there was an improper representation of a by x_0, y_0. Let $g = \gcd(x_0, y_0)$. Since the representation is improper, $g > 1$. We see that

$$\begin{aligned} f\left(\frac{x_0}{g}, \frac{y_0}{g}\right) &= a\left(\frac{x_0}{g}\right)^2 + b\left(\frac{x_0}{g}\cdot\frac{y_0}{g}\right) + c\left(\frac{y_0}{g}\right)^2 \\ &= \frac{1}{g^2}\cdot a\left(x_0\right)^2 + \frac{1}{g^2}\cdot b\left(x_0\cdot y_0\right) + \frac{1}{g^2}\cdot c\left(y_0\right)^2 \\ &= \frac{1}{g^2}\left(ax_0^2 + bx_0y_0 + cy_0^2\right) \\ &= \frac{1}{g^2} f(x_0, y_0) \\ &= \frac{a}{g^2}. \end{aligned}$$

By theorem 1.7, $\gcd\left(\frac{x_0}{g}, \frac{y_0}{g}\right) = 1$. So $\frac{a}{g^2}$ is properly represented by f and $\frac{a}{g^2} < a$ given that $g > 1$. We've arrived at a contradiction. Thus, there cannot be a improper representation of a. Since a is represented by f, it can only be represented properly. $\square$

Problem (3.7.2)

Let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced positive definite form. Show that improper represents of c may exist.

Solution.

Suppose $c = r^2a$ for $r \in \mathbb{Z}$ and $r > 1$. If $f(x_0, y_0) = a$, then $\gcd(x_0, y_0) = 1$ because all representations of a by f are proper. By theorem 1.6, we see that $\gcd(rx_0, ry_0) = r$. But $f(rx_0, ry_0) = r^2a = c$. Thus, improper representations of c may exist when $c = r^2a$ for some integer r greater than 1. $\square$

Problem (3.7.3)

Show that any positive definite binary quadratic form of discriminant -3 is equivalent to $f(x,y) = x^2 + xy + y^2$. Show that a positive integer n is properly represented by f if and only if n is of the form $n = 3^\alpha \prod p^\beta$, where $\alpha = 0$ or 1 and all the primes p are of the form $3k+1$. ~~Show that for n of the form, $r_f(n) = 6 \cdot 2^s$, where s is the number of distince primes $p \equiv 1 \mod 3$ that divide n.~~.

Solution.

First we show that positive definite binary quadratic form of discriminant -3 is equivlent to $f(x,y) = x^2 + xy + y^2$. By theorem 3.18, any binary quadratic form is equivalent to some reduced binary quadratic form. By theorem 3.17, two equivalent binary quadratic forms will have the same discriminant. By theorem 3.19, a reduced positive definite binary quadratic form is subject to the restriction $0 < a \leq \sqrt{-d/3}$.

Let $h(x,y) = ax^2+bxy+cy^2$. Putting this together, there is some reduced binary quadratic form equivalent to h, which we will call $g(x,y) = Ax^2 + Bxy + Cy^2$, such that $d = b^2 - 4ac = B^2 - 4AC = D$ and $0 < A \leq \sqrt{-D/3} = \sqrt{3/3} = 1$. Since g is reduced, we see that $-|A| < B \leq |A| < |C|$ or $0 \leq B \leq |A| < |C|$. Either way, we see that B can only take on the values of 0 or 1. If $B = 0$, then $D = -4AC \equiv 0 \not\equiv -3 = D \mod 4$, so $B \neq 0$. If $A = B = 1$, then

$$\begin{aligned} -3 &= D \\ -3 &= B^2 - 4AC \\ -3 &= 1^2 - 4 \cdot 1 \cdot C \\ -4 &= -4C \\ 1 &= C. \end{aligned}$$

We see that $A = B = C$ so $g(x,y) = x^2 + xy + y^2$. Thus, h is equivalent to $x^2 + xy + y^2$.

Next we show that a positive integer n is properly represented by f if and only if n is of the form $n = 3^\alpha \prod p^\beta$, where $\alpha = 0$ or 1 and all the primes p are of the form $3k+1$.

Theorem 3.13 tells us that f will properly represent n if the congruence

$$x^2 \equiv d \mod 4|n| \tag{1}$$

has a solution. Given $d = -3$ and $n > 0$ we may rewrite equation 1 as

$$x^2 \equiv -3 \mod 4n. \tag{2}$$

First we show that f cannot properly represent an even number. Suppose $\gcd(x_0, y_0) = 1$. Then $2 \mid x_0$ or $2 \mid y_0$ or neither. Suppose that x_0 is even and y_0 is odd. Then $f(x_0, y_0) = x_0^2 + x_0 y_0 + y_0^2$, which is odd because $x_0^2 + x_0 y_0$ is even but y_0^2 is odd. The case where x_0 is even and y_0 is odd makes $f(x_0, y_0)$ odd by a symmetrical argument. So 2 does not appear in the prime factorization of n.

Let us write $n = 3^\alpha \prod_{p|n} p^\beta$ as permitted by the fundamental theorem of arithmetic, where $p > 3$ and $\alpha \in \mathbb{N}$. By the chinese remainder theorem, equation 2 can be rewritten as

$$x^2 \equiv -3 \mod 4 \cdot 3^\alpha \cdot \prod_{\substack{p|n \\ p>3}} p^\beta. \tag{3}$$

It is clear that $\gcd\left(4, 3^\alpha, \prod p^\beta\right) = 1$. By the chinese remainder theorem, we see that a solution will exist to equation 3 if and only if solutions exist to the following three congruences:

$$x^2 \equiv -3 \mod 4 \tag{4}$$

$$x^2 \equiv -3 \mod 3^\alpha \tag{5}$$

$$x^2 \equiv -3 \mod \prod_{\substack{p|n \\ p>3}} p^\beta. \tag{6}$$

We see that equation 4 is true because $x^2 \equiv -3 \equiv 1 \mod 4$ and 1 is a perfect square.

For equation 5 we will prove that the congruence

$$x^2 \equiv -p \mod p^\alpha \tag{7}$$

where p is prime only has solutions for $\alpha = 0$ or 1.

First we examine the case where $\alpha = 0$ so $p^\alpha = p^0 = 1$. Since every integer is divisible by 1, $1 \mid (x^2 + p)$ so $x^2 \equiv -p \mod 1$.

Now we consider the case where $\alpha = 1$. We see that $x^2 \equiv -p \equiv 0 \mod p$ is trivially true.

Next we consider the case where $\alpha > 1$. To start, we note that $x^2 \equiv -p \mod p^\alpha$ if and only if $x^2 = -p + np^\alpha$ for $n \in \mathbb{Z}$ where $n \neq 0$ because p is not a perfect square. We see that $-p + np^\alpha = p(-1 + np^{\alpha-1})$. By the fundamental theorem of arithmetic, we see that any number squared will have even exponents among its prime factors. Thus, $(-1 + np^{\alpha-1})$ must contain p in its prime factorization and the exponent must be odd, so $p \mid (-1 + np^{\alpha-1})$. But $p \mid np^{\alpha-1}$, so if $p \mid (-1 + np^{\alpha-1})$ then

$$\begin{aligned} p &\mid -(-1 + np^{\alpha-1}) + np^{\alpha-1} \\ p &\mid 1. \end{aligned}$$

Since no prime number can divide 1, no solution to equation 7 can exist for $\alpha > 1$. Setting $p = 3$ in equation 7 gives us equation 5. Thus, $\alpha = 0$ or $\alpha = 1$.

We use Legendre symbols to find the solutions to equation 6. By the chinese remainder theorem, equation 6 will have a solution if and only if the congruence

$$x^2 \equiv -3 \mod p^\beta$$

is true for each $p \mid n$ such that $p^\beta \parallel n$ and $p > 3$. We see that each congruence of this form requires that

$$x^2 \equiv -3 \mod p$$

is true as well. If this has a solution, then if $f(x) = x^2 + 3$ has a solution $f(x_0) = 0$, and $f'(x_0) = 2x_0 \not\equiv 0 \mod p$, Hansel's lemma tells us that congruence $x^2 \equiv -3 \mod p^\beta$ will have a solution. Let us call $p = \gamma$. We have

$$\left(\frac{-3}{\gamma}\right) = \left(\frac{-1}{\gamma}\right)\left(\frac{3}{\gamma}\right).$$

We have two cases

(1) $\gamma \equiv 1 \mod 4$:
We see that

$$\begin{aligned}\left(\frac{-1}{\gamma}\right) &= (-1)^{\frac{\gamma-1}{2}} \\ &= 1,\end{aligned}$$

Furthermore, we see that

$$\begin{aligned}\left(\frac{3}{\gamma}\right) &= \left(\frac{\gamma}{3}\right) && \text{by quadratic reciprocity} \\ &= \begin{cases} 1 & \gamma \equiv 1 \mod 3 \\ -1 & \gamma \equiv 2 \mod 3 \end{cases}\end{aligned}$$

Putting this together, we see that

$$\left(\frac{-1}{\gamma}\right)\left(\frac{3}{\gamma}\right). = \begin{cases} 1 & \gamma \equiv 1 \mod 3 \\ -1 & \gamma \equiv 2 \mod 3 \end{cases}$$

(2) $\gamma \equiv 3 \mod 4$:
We see that

$$\begin{aligned}\left(\frac{-1}{\gamma}\right) &= (-1)^{\frac{\gamma-1}{2}} \\ &= -1,\end{aligned}$$

Furthermore, we see that

$$\begin{aligned}\left(\frac{3}{\gamma}\right) &= -\left(\frac{\gamma}{3}\right) && \text{by quadratic reciprocity} \\ &= \begin{cases} -1 & \gamma \equiv 1 \mod 3 \\ 1 & \gamma \equiv 2 \mod 3 \end{cases}\end{aligned}$$

Putting this together, we see that

$$\left(\frac{-1}{\gamma}\right)\left(\frac{3}{\gamma}\right). = \begin{cases} 1 & \gamma \equiv 1 \mod 3 \\ -1 & \gamma \equiv 2 \mod 3 \end{cases}$$

In each case, we see that $\left(\frac{-3}{\gamma}\right) = 1$ when $\gamma \equiv 1 \mod 3$ and $\left(\frac{-3}{\gamma}\right) = -1$ otherwise. Thus, solutions will exist to $x^2 \equiv -3 \mod p^\beta$ if and only if $p \equiv 1 \mod 3$. If $p \equiv 1 \mod 3$ for every $p \mid n$ such that $p > 3$, then we can use the chinese remainder theorem to find a solution to equation 6.

Putting this all together, we see thata n will be properly represented by f if and only if equation 2 is true. We showed that $2 \nmid n$ and that $3||n$ or $3 \nmid n$, and equation 2 can be rewritten as equation 3. We showed that equation 3 is true if and only if equations 4, 5, and 6 are true. We showed that equations 4 is true unconditionally and that equation 5 is true for $\alpha = 0$ or 1. Furthermore, we showed that equation 6 is true if every prime dividing n greater than 3 is congruent to 1 modulo 3. $\square$

Problem (3.7.5)

Show that for any given $d < 0$, the primitive positive definite quadratic forms of discriminant d all have the same number of automorphs.

Solution.

From theorem 3.26, we see that the number of automorphs can only be 2, 4, or 6. We denote the number of automorphs of a binary quadratic form, f, by $w(f)$. Let $f(x, y) = ax^2 + bxy + cy^2$ be a primitive positive definite binary quadratic form of discriminant d. We consider two cases

(1) $w(f) = 4$:
Theorem 3.26 tells us that $a = c$ and $b = 0$. We require that $\gcd(a, b, c) = 1$ because f is primitive. We see that this requires $a = c = 1$. From this we see that $d = b^2 - 4ac = 0^2 - 4 \cdot 1 \cdot 1 = -4$. Since d is not a perfect square, we can use theorem 3.19 to find the reduced binary quadratic forms of those with discriminant $d = -4$.

By theorem 3.18, there will be at least one reduced binary quadratic form with discriminant d for every equivalence class. Let $g(x, y) = Ax^2 + Bxy + Cy^2$ be a positive definite reduced binary quadratic form with discriminant $D = d = -4$. We see that $0 < A \leq \sqrt{-d/3} = \sqrt{4/3} < \sqrt{12/3} = \sqrt{4} = 2$. So $A = 1$. Since $-1 = -|A| < B \leq |A| = 1 < C$ or $0 \leq B \leq |A| = |C|$, we see that $B = 0$ or $B = 1$. Since $D \equiv 0 \mod 4$, we see that $B \neq 1$ because then $D = B^2 - 4AC = 1^2 - 4AC \not\equiv 0 \mod 4$. Thus, $B = 0$. Now we can solve for C using $D = -4$.

$$\begin{aligned} D &= B^2 - 4AC \\ -4 &= 0^2 - 4 \cdot 1 \cdot C \\ -4 &= -4 \cdot C \\ 1 &= C. \end{aligned}$$

Thus $A = C = 1$ and $B = 0$. So we see that there is only one reduced positive definite binary quadratic form with discriminant $d = -4$. Thus, there is only one equivalence class so all binary quadratic forms of discriminant $d = -4$ are equivalent.

By theorem 3.26, equivalent positive definite binary quadratic forms have the same number of automorphs. Thus, every primitive positive definite binary quadratic form of discriminant $d = -4$ is equivalent to g, which has 4 automorphs.

(2) $w(f) = 6$:
By theorem 3.26, $a = b = c$. Given that $\gcd(a, b, c) = 1$ because f is primitive, we see that $a = b = c = 1$. From this we see that $d = b^2 - 4ac = 1^2 - 4 \cdot 1 \cdot 1 = -3$. Since d is not a perfect square, we can use theorem 3.19 to find the reduced binary quadratic forms of those with discriminant $d = -3$.

By theorem 3.18, there will be at least one reduced binary quadratic form with discriminant d for every equivalence class. Let $g(x, y) = Ax^2 + Bxy + Cy^2$ be a positive definite reduced binary quadratic form with discriminant $D = d = -3$. We see that $0 < A \leq \sqrt{-d/3} = \sqrt{1} = 1$. Since $-1 = -|A| < B \leq |A| = 1 < C$ or $0 \leq B \leq |A| = |C|$, we see that $B = 0$ or $B = 1$. Since $D \equiv 1 \mod 4$, $B \neq 0$ because then $D = B^2 - 4AC = 0^2 - 4AC \equiv 0 \mod 4$. Thus, $B = 1$. Now we can solve for

C using $D = -3$.

$$\begin{aligned} D &= B^2 - 4AC \\ -3 &= 1^2 - 4 \cdot 1 \cdot C \\ -4 &= -4 \cdot C \\ 1 &= C. \end{aligned}$$

So we see that there is only one reduced positive definite binary quadratic form with discriminant $d = -3$. Thus, there is only one equivalence class so all binary quadratic forms of discriminant $d = -3$ are equivalent.

By theorem 3.26, equivalent positive definite binary quadratic forms have the same number of automorphs. Thus, every primitive positive definite binary quadratic form of discrimiant $d = -3$ is equivalent to g, which has 6 automorphs.

So far we have showed that if $d = -3$ or $d = -4$, then f will be equivalent to a reduced positive definite binary quadratic form with a known number of automorphs. Since the number of automorphs of two equivalent binary quadratic forms are equal, we see that $w(f) = 4$ if and only if $d = -4$ and $w(f) = 6$ if and only if $d = -3$. For all other primitive binary quadratic forms of discriminant $d \neq -3$ and $d \neq -4$, the number of automorphs must be 2 because f cannot be equivalent to the only two known reduced binary quadratic forms with a number of automorphs greater than 2 because equal discriminants is a necessary condition for equivalence. $\square$

Problem (4.1.2)

If 100! were written out in the orginary decimal notation without the factorial sign, how many zeros would there be in a row at the right end?

Solution.

The decimal representation of a number n will end in a 0 if $10 \mid n$. Furthermore, the number of 0's that trail the decimal representation of n is equal to the highest power of 10 that divides n. But 10 can be factored as $2 \cdot 5$, so the highest power of 10 that divides n is the minimum of the highest power that 2 can divide n and the highest power of 5 that can divide n.

By theorem 4.2, we see that $2^{e_1} \parallel 100!$ where

$$\begin{aligned} e_1 &= \sum_{i=1}^{\infty} \left\lfloor \frac{100}{2^i} \right\rfloor \\ &= \sum_{i=1}^{6} \left\lfloor \frac{100}{2^i} \right\rfloor \\ &= \left\lfloor \frac{100}{2^1} \right\rfloor + \left\lfloor \frac{100}{2^2} \right\rfloor + \left\lfloor \frac{100}{2^3} \right\rfloor + \left\lfloor \frac{100}{2^4} \right\rfloor + \left\lfloor \frac{100}{2^5} \right\rfloor + \left\lfloor \frac{100}{2^6} \right\rfloor \\ &= 50 + 25 + 12 + 6 + 3 + 1 \\ &= 97 \end{aligned}$$

Likewise, we see that $5^{e_2} \parallel 100!$ where

$$\begin{aligned} e_2 &= \sum_{i=1}^{\infty} \left\lfloor \frac{100}{5^i} \right\rfloor \\ &= \sum_{i=1}^{2} \left\lfloor \frac{100}{5^i} \right\rfloor \\ &= \left\lfloor \frac{100}{5^1} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor \\ &= 20 + 4 \\ &= 24 \end{aligned}$$

We see that $\min(97, 24) = 24$, so $10^{24} \parallel 100!$, so the decimal representation of 100! has 24 trailing 0's. $\square$

Problem (4.1.4)

Given that $[x+y] = [x] + [y]$ and $[-x-y] = [-x] + [-y]$, prove that x or y is an integer.

Solution.

Let $x = u + v$, where $u \in \mathbb{Z}$ and $0 \leq v < 1$, and let $y = r + s$, where $r \in \mathbb{Z}$ and $0 \leq s < 1$. We see that

$$\begin{aligned}[x] + [y] &= u + r \\ &\leq [u + v + r + s] = [x + y] \\ &= [u + r] + [v + s] \\ &= (u + r) + [v + s].\end{aligned}$$

We are given $[x] + [y] = [x + y]$ so we see that $[v + s] = 0$, which is true when $0 \leq v + s < 1$.

We see that $-x = -u - v = -u - 1 + (1 - v)$ and that $-y = -r - s = -r - 1 + (1 - s)$ where $0 < 1 - v, 1 - s \leq 1$. Suppose for the sake of contradiction that $v \neq 0$ and $r \neq 0$. We see that

$$\begin{aligned}[-x] + [-y] &= -u - 1 - r - 1 \\ &\leq [-u - 1 + (1 - v) - r - 1 + (1 - s)] = [-x - y] \\ &= [-u - 1 - r - 1] + [1 - v + 1 - s].\end{aligned}$$

Here we see that $[-x] + [-y] = [-x - y]$ requires $[1 - v + 1 - s] = 0$. This is true when

$$\begin{aligned}0 \leq 1 - v + 1 - s &< 1 \\ 0 \leq 2 - v - s &< 1 \\ -2 \leq -v - s &< -1 \\ 2 \geq v + s &> 1.\end{aligned}$$

This is a contradiction, as the quantity $v + s$ cannot be both strictly greater than and stricly less than 1. Thus, $v = 0$ or $r = 0$. If $v = 0$, then $x = u \in \mathbb{Z}$ and x is an integer. Likewise, if $s = 0$, then $y = s \in \mathbb{Z}$ and y is an integer. $\square$

Problem (4.1.6)

For any real number x prove that $[x] + \left[x + \frac{1}{2}\right] = [2x]$.

Solution.

Let $x = u + v$, where $u \in \mathbb{Z}$ and $0 \leq v < 1$. Let $f(x) = [x] + \left[x + \frac{1}{2}\right]$ and $g(x) = [2x]$. We see that

$$\begin{aligned} f(x) &= [x] + \left[x + \frac{1}{2}\right] \\ &= [u + v] + \left[u + v + \frac{1}{2}\right] \\ &= u + u + \left[v + \frac{1}{2}\right] \\ &= \begin{cases} 2u & v < \frac{1}{2} \\ 2u + 1 & v \geq \frac{1}{2} \end{cases} \end{aligned}$$

We also see that

$$\begin{aligned} g(x) &= [2x] \\ &= [2u + 2v] \\ &= 2u + [2v] \\ &= \begin{cases} 2u & v < \frac{1}{2} \\ 2u + 1 & v \geq \frac{1}{2} \end{cases} \end{aligned}$$

We see that $f \equiv g$, or f is identically equal to g. Thus, $[x] + \left[x + \frac{1}{2}\right] = [2x]$. □

Problem (4.1.9)

Prove that $(2n)!/(n!)^2$ is even if n is a positive integer.

Solution.

First we aim to show that the quantity $(2n)!/(n!)^2$ is a positive integer. Using theorem 4.2, we see that $(2n)!/(n!)^2 \in \mathbb{Z}$ if in the prime factorization of the numerator and denominator, the numerator contains the same prime factors as in the denominator with equal or larger exponents. It will be sufficient to show that for an arbitrary prime p, and exponents $e_1, e_2 \in \mathbb{N}$, if $p^{e_1} \parallel (2n)!$ and $p^{e_2} \parallel (n!)^2$, then $e_1 \geq e_2$.

Using theorem 4.2, we see that

$$e_1 = \sum_{i=1}^{\infty} \left[\frac{2n}{p^i} \right]$$

and

$$e_2 = 2 \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right],$$

where the coefficient 2 comes from the fact that squaring a number doubles the value of each exponent in its prime factorization.

From theorem 4.1(4), we see that

$$\begin{aligned} e_2 &= 2 \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right] \\ &= \sum_{i=1}^{\infty} \left(\left[\frac{n}{p^i} \right] + \left[\frac{n}{p^i} \right] \right) \\ &\leq \sum_{i=1}^{\infty} \left[\frac{n}{p^i} + \frac{n}{p^i} \right] && \text{by theorem 4.1(4)} \\ &= \sum_{i=1}^{\infty} \left[\frac{2n}{p^i} \right] \\ &= e_1. \end{aligned}$$

Of course, the factorial is alwyas positive, to the the quantity $(2n)!/(n!)^2$ will be positive. This proves our first assertion: that $(2n)!/(n!)^2 \in \mathbb{Z}^+$

To show that $(2n)!/(n!)^2$ is even, we only need to show that if $p = 2$, that $e_1 > e_2$. First we show that $\sum_{i=1}^{\infty} \left[\frac{n}{2^i} \right] < n$. We see that

$$\sum_{i=1}^{\infty} \left[\frac{n}{2^i} \right] = \sum_{\substack{i=1 \\ 2^i \leq n}} \left[\frac{n}{2^i} \right] + \sum_{\substack{i \\ 2^i > n}} \left[\frac{n}{2^i} \right]$$

$$
\begin{aligned}
&= \sum_{\substack{i=1 \\ 2^i \le n}} \left\lceil \frac{n}{2^i} \right\rceil \\
&\le \sum_{\substack{i=1 \\ 2^i \le n}} \frac{n}{2^i} && \text{by theorem 4.1(1)} \\
&< \sum_{\substack{i=1 \\ 2^i \le n}} \frac{n}{2^i} + \sum_{\substack{i \\ 2^i > n}} \frac{n}{2^i} \\
&= \sum_{i=1} \frac{n}{2^i} \\
&= n \sum_{i=1} \frac{1}{2^i} \\
&= n.
\end{aligned}
$$

We can use this result to show

$$
\begin{aligned}
e_2 &= 2 \sum_{i=1}^{\infty} \left\lceil \frac{n}{2^i} \right\rceil \\
&= \sum_{i=1}^{\infty} \left\lceil \frac{n}{2^i} \right\rceil + \sum_{i=1}^{\infty} \left\lceil \frac{n}{2^i} \right\rceil \\
&< n + \sum_{i=1}^{\infty} \left\lceil \frac{n}{2^i} \right\rceil \\
&= \left\lceil \frac{2n}{2^1} \right\rceil + \sum_{i=1}^{\infty} \left\lceil \frac{2n}{2^{i+1}} \right\rceil \\
&= \left\lceil \frac{2n}{2^1} \right\rceil + \sum_{i=2}^{\infty} \left\lceil \frac{2n}{2^i} \right\rceil \\
&= \sum_{i=1}^{\infty} \left\lceil \frac{2n}{2^i} \right\rceil \\
&= e_1.
\end{aligned}
$$

Since $e_1 > e_2$, we can always factor out a 2 from the numerator of the integer $(2n)!/(n!)^2$. Since $(2n)!/(n!)^2$ is a positive integer for all $n \in \mathbb{N}$ and is always even, we are done. $\square$

Problem (4.2.2)

Find the smallest integer x for which $d(x) = 6$.

Solution.

From theorem 4.3, we see that $d(x) = \prod_{p^\alpha \| x}(\alpha + 1)$. It is easy to see that the only ways to factor 6 are as $1 \cdot 6$ and $2 \cdot 3$. Since d is multiplicitive, we can $d(x) = 6$ in two cases: x has one prime factor to the fifth power; or x has two prime factors, one to the first power and one to the second power. We examine both cases:

(1) $\omega(x) = 1$:
    We see that $x = p_1^5$. The smallest number of this form is $x = 2^5 = 32$.
(2) $\omega(x) = 2$:
    We see that $x = p_1 p_2^2$. The smallest number of this form is $x = 3 \cdot 2^2 = 12$.

Since we have covered all cases and the smallest number among them was $x = 12$, we see that the smallest number such that $d(x) = 6$ is 12. □

Problem (4.2.5)

Prove that $\prod_{d|n} d = n^{d(n)/2}$.

Solution.

We have two cases:

(1) n is a not a perfect square:
Clearly, if $d \mid n$ for some $d \in \mathbb{Z}^+$, then $\frac{n}{d} \in \mathbb{Z}$ and $\frac{n}{d} \Big| n$. Furthermore, $d \neq \frac{n}{d}$ because $n \neq d^2$ for any d. For every divisor d of n, there is another distinct divisor $\frac{n}{d}$ such that $d \cdot \frac{n}{d} = n$. Since we can pair every divisor of n with another divisor of n in this way, there are $\frac{d(n)}{2}$ of these pairs. We see that

$$\begin{aligned}\prod_{d|n} d &= \prod_{\substack{d|n \\ d<\sqrt{n}}} d \cdot \frac{n}{d} \\ &= \prod_{\substack{d|n \\ d<\sqrt{n}}} n \\ &= n^{d(n)/2},\end{aligned}$$

so we are done.

(2) n is a perfect square:
Likewise, if $d \mid n$ for some $d \in \mathbb{Z}^+$, then $\frac{n}{d} \in \mathbb{Z}$ and $\frac{n}{d} \Big| n$. However, there is exactly one divisor such that $d = \frac{n}{d}$ because $n = d^2$ for some d. For every other divisor d of n, where $d \neq \sqrt{n}$, there is another distinct divisor $\frac{n}{d}$ such that $d \cdot \frac{n}{d} = n$. There are $\frac{d(n)-1}{2}$ of these pairs. We see that

$$\begin{aligned}\prod_{d|n} d &= n^{1/2} \cdot \prod_{\substack{d|n \\ d<\sqrt{n}}} d \cdot \frac{n}{d} \\ &= n^{1/2} \cdot \prod_{\substack{d|n \\ d<\sqrt{n}}} n \\ &= n^{1/2} \cdot n^{\frac{d(n)-1}{2}} \\ &= n^{\frac{d(n)-1}{2}+\frac{1}{2}} \\ &= n^{d(n)/2},\end{aligned}$$

so we are done.

□

Problem (4.2.6)

Prove that $\sum_{d|n} d = \sum_{d|n} n/d$, and more generally that $\sum_{d|n} f(d) = \sum_{d|n} f(n/d)$.

Solution.

Let D_n denote the set of divisors of n. We will show that the function $g : D_n \to D_n$ where $g(x) = \frac{n}{x}$ is a permutation of the set D_n. It suffices to show that g is bijective. We see that if $g(d_1) = g(d_2)$, then

$$\begin{aligned} \frac{n}{d_1} &= \frac{n}{d_2} \\ d_2 &= d_1, \end{aligned}$$

so g is injective. Next we see that if $d \in D_n$, then

$$\begin{aligned} g\left(\frac{n}{d}\right) &= \left(\frac{n}{\left(\frac{n}{d}\right)}\right) \\ &= d. \end{aligned}$$

Clearly $\frac{n}{d} \in D_n$ because $\frac{n}{d} \cdot d = n$ so $\frac{n}{d} \big| n$. So g is surjective.

Since g is injective and surjective, g is bijective. A bijective function whose domain and range are the same set is a permutation. Thus g is permutation on D_n.

Now it should be clear that

$$\sum_{d|n} f(d) = \sum_{d|n} f(n/d),$$

because we are calling f on all members of the set D_n, and addition is commutative. We see that

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} f(g(d)) \\ &= \sum_{d|n} f\left(\frac{n}{d}\right). \end{aligned}$$

Furthermore, when f is the identity function, we get

$$\sum_{d|n} d = \sum_{d|n} \frac{n}{d},$$

completing the proof. □

Problem (4.2.12)

Prove that the number of divisors of n is odd if and only if n is a perfect square. If the integer $k \geq 1$, prove that $\sigma_k(n)$ is odd if and only if n is a square or double a square.

Solution.

First we aim to show that $d(n)$ is odd if and only if n is a perfect square. From theorem 4.3, we see that

$$d(n) = \prod_{p^\alpha \| n} (\alpha + 1).$$

If $\alpha + 1$ were even for any α, then $d(n)$ would be even. Furthermore, we see that if α is even for each prime p, that $d(n)$ will be odd. Thus, $d(n)$ is odd if and only if each α is even. By the fundamental theorem of arithmetic, we can factor n in the product of prime powers. It should be clear that all the exponents will be even if and only if n is a perfect square. Thus, $d(n)$ is odd if and only if n is a perfect square.

Next we aim to show that for an integer $k \geq 1$, then $\sigma_k(n)$ is odd if and only if n is a square or double a square. By definition, $\sigma_k(n) = \sum_{d|n} d^k$. We see that for any $k \geq 1$ and $d \in \mathbb{Z}^+$, that $d^k \equiv d \mod 2$. Thus,

$$\begin{aligned} \sigma_k(n) &= \sum_{d|n} d^k \\ &\equiv \sum_{d|n} d \mod 2 \\ &= \sigma(n). \end{aligned}$$

We see that it is sufficient to show that $\sigma(n)$ is odd if and only if n is a square or double a square.

We know that $\sigma(n)$ is multiplicitive and that $\sigma(p^k) = 1 + p + p^2 + \cdots + p^k$. Suppose that n can be factored as $\prod p^\alpha$. We see that

$$\begin{aligned} \sigma(n) &= \sigma\left(\prod_p p^\alpha\right) \\ &= \prod_p \sigma(p^\alpha) \\ &= \prod_p \left(\sum_{i=1}^{\alpha} p^i\right). \end{aligned}$$

Thus, we see that $\sigma(n)$ will be odd ($\sum_{i=1}^{\alpha} p^i$) is odd for each prime p such that $p^\alpha \| n$. We have two cases:

(1) $p = 2$:
We see that

$$\sum_{i=1}^{\alpha} 2^i = \frac{2^{\alpha+1} - 1}{2 - 1}$$

$$= 2^{\alpha+1} - 1$$
$$\equiv 1 \mod 2,$$

so $\sum_{i=1}^{\alpha} 2^i$ is always odd.

(2) $p \neq 2$:
Since the only even prime is 2, we see that p must be odd. Thus, p^k is odd for every $k \in \mathbb{N}$. Clearly, $\sum_{i=1}^{\alpha} p^i$ has $\alpha + 1$ terms, all odd. Thus, the quantity will only be odd when α is even.

Putting this together, we see that $\sigma(n)$ is odd when every odd prime p such that $p \mid n$ has an even exponent in the prime factorization of n. If the exponent of 2 in the prime factorization of n is even, then clearly n is a perfect square. Otherwise, we can factor out a 2 and write n as 2 times a perfect square.

Thus, $\sigma_k(n)$ is odd if and only if $\sigma(n)$ is odd. And $\sigma(n)$ is odd if and only if n is a perfect square or twice a perfect square, completing the proof. $\square$

Problem (4.2.16)

We say (following Euclid) that m is a perfect number if $\sigma(m) = 2m$, that is, if m is the sum of all its positive divisors other than itself. If $2^n - 1$ is a prime p, prove that $2^{n-1}p$ is a perfect number. Use this result to find three perfect number.

Solution.

We see that

$$\begin{aligned}
\sigma(2^{n-1}p) &= \sigma(2^{n-1})\sigma(p) \\
&= \frac{2^{(n-1)+1} - 1}{2 - 1}(1 + p) \\
&= (2^n - 1)(1 + p) \\
&= p(1 + p) \\
&= p \cdot 2^n \\
&= 2 \cdot 2^{n-1}p.
\end{aligned}$$

By definition $2^{n-1}p$ is a perfect number.

We see that

$$\begin{aligned}
3 &= 2^2 - 1 \\
7 &= 2^3 - 1 \\
31 &= 2^5 - 1.
\end{aligned}$$

Thus, we can find three perfect numbers

$$\begin{aligned}
3 \cdot 2^{2-1} &= 3 \cdot 2 = 6 \\
7 \cdot 2^{3-1} &= 7 \cdot 4 = 28 \\
31 \cdot 2^{5-1} &= 31 \cdot 16 = 496.
\end{aligned}$$

So 6, 28, and 496 are three perfect numbers. □

Problem (4.3.1)

Find a positive integer n such that $\mu(n) + \mu(n+1) + \mu(n+2) = 3$.

Solution.

By definition, $\mu(n) = (-1)^{\omega(n)}$, where $\omega(n)$ is the number of distinct primes dividing n. We see that $n = 20$ has the given property. Notice that $20 = 2^2 \cdot 5$, that $21 = 3 \cdot 7$, and that $22 = 2 \cdot 11$. Thus $\omega(20) = \omega(21) = \omega(22) = (-1)^2 = 1$. Thus, we see that $\mu(20) + \mu(21) + \mu(22) = 3$. □

Problem (4.3.5)

Prove that for every positive integer n, $\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$.

Solution.

By definition, $\mu(n) = (-1)^{\omega(n)}$, where $\omega(n)$ is the number of distinct primes dividing n if n is square free and 0 otherwise. We see that there are $\sum_{d|n} |\mu(d)|$ square free divisors of n.

Since there are $\omega(n)$ distinct primes dividing n, there are $\binom{\omega(n)}{k}$ square free divisors of n with k factors. Thus, there are $\sum_{k=0}^{\omega(n)} \binom{\omega(n)}{k}$ square free divisors of n. By the binomial theorem, we see that

$$\begin{aligned}\sum_{k=0}^{\omega(n)} \binom{\omega(n)}{k} &= (1+1)^{\omega(n)} \\ &= 2^{\omega(n)}\end{aligned}$$

square free divisors of n. Thus, $2^{\omega(n)} = \sum_{d|n} |\mu(d)|$ and we are done. $\square$