18.781
PROBLEM SET 7

JOHN WANG

1. Problem 1

Problem 1.1. *Let n be a positive integer. Evaluate $\sum_{k=0}^{n} \binom{n}{3k}$.*

Solution First, we know that $(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k$ is the generating function for the expression. Let us now use the third roots of unity ω and substitute them into the expression for the generating function. We know that the third roots of unity are 1 and $-\frac{1}{2} \pm \frac{i\sqrt{3}}{2}$. Moreover, we know that the following holds, using the fact that $\omega^2 = -\omega - 1$:

$$\sum_{k=0}^{n} \omega^k \binom{n}{k} = (1+\omega)^n = (-\omega^2)^n \tag{1.1}$$

$$\sum_{k=0}^{n} \omega^{2k} \binom{n}{k} = (1+\omega^2)^n = (-\omega)^n \tag{1.2}$$

$$\sum_{k=0}^{n} 1^k \binom{n}{k} = (1+1)^n = 2^n \tag{1.3}$$

Therefore, since we know that summing up each of these series, we will obtain the sum $3\sum_{k=0}^{n} \binom{n}{3k}$, we find that:

$$3\sum_{k=0}^{n} \binom{n}{3k} = 2^n + (-\omega)^n + (-\omega)^{2n} \tag{1.4}$$

$$\sum_{k=0}^{n} \binom{n}{3k} = \frac{1}{3}\left(2^n + (-\omega)^n + (-\omega)^{2n}\right) \tag{1.5}$$

The completes the calculation. □

2. Problem 2

For a sequence $\{a_n\}$ we can define another kind of generating function called an exponential generating function as follows:

$$\bar{A}(x) = \sum_{n \geq 0} a_n \frac{x^n}{n!}. \tag{2.1}$$

It satisfies many of the nice properties we have seen for generating functions (for example, linearity with respect to the sequence). But some properties are slightly modified.

Problem 2.1. *Show that the generating function for the left-shifted sequence $\{a_1, a_2, \ldots\}$ is $\frac{d}{dx}\bar{A}(x)$.*

Solution We see that if we differentiate $\bar{A}(x)$, we obtain the following:

$$\frac{d}{dx}\bar{A}(x) = \sum_{n \geq 0} a_n \frac{d}{dx}\frac{x^n}{n!} \tag{2.2}$$

$$= \sum_{n \geq 0} a_n \frac{nx^{n-1}}{n!} \tag{2.3}$$

$$= \sum_{n \geq 0} a_n \frac{x^{n-1}}{(n-1)!} \tag{2.4}$$

$$= \sum_{n \geq 1} a_n \frac{x^n}{n!} \tag{2.5}$$

This is exactly what we wanted to show because the bottom expression is the sequence $\{a_n\}$ left shifted by one unit. $\square$

Problem 2.2. *If $\bar{A}(x)$ is the exponential generating function for $\{a_n\}$ and $\bar{B}(x)$ is the exponential generating function for $\{b_n\}$, show that $\bar{A}(x)\bar{B}(x)$ is the exponential generating function for the sequence $\{c_n\}$ given by $c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$.*

Solution We shall compute $\bar{A}(x)\bar{B}(x)$ by examining the coefficients of $\frac{x^n}{n!}$ for each $n \geq 0$. We see that if we multiply the terms on a_k and b_{n-k} we obtain:

$$a_k \frac{x^k}{k!} b^{n-k} \frac{x^{n-k}}{(n-k)!} = a_k b_{n-k} \frac{x^n}{k!(n-k!)} \tag{2.6}$$

Moreover, we know that the only terms that have x^n are those where $k + (n-k) = n$. This includes all k ranging from 0 to n. However, we know that in the exponential generating function, we must have $\frac{x^n}{n!}$ as the term without the coefficient c_n. However, we know that $\frac{x^n}{n!}\binom{n}{k} = \frac{x^n}{k!(n-k)!}$. Therefore, we know

$$a_k b_{n-k} \frac{x^n}{k!(n-k)!} = \binom{n}{k} a_k b_{n-k} \frac{x^n}{n!} \tag{2.7}$$

Since we range over all $k \in \{0, 1, \ldots, n\}$, we see that $c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$ as desired. $\square$

Problem 2.3. *Show that the generating function $E(x)$ for the sequence $a_n = r^n$ (where r is some fixed complex number) satisfies $E'(x) = rE(x)$. Solve this differential equation to deduce that $e^{rx} = \sum_{n\geq 0} \frac{r^n x^n}{n!}$.*

Solution We know that $E(x) = 1 + rx + r^2 + \frac{x^2}{2!} + \ldots = \sum_{n\geq 0} r^n \frac{x^n}{n!}$. Taking the derivative we find:

$$E'(x) = \sum_{n\geq 0} r^n \frac{d}{dx}\frac{x^n}{n!} \tag{2.8}$$

$$= \sum_{n\geq 1} r^n \frac{x^{n-1}}{(n-1)!} \tag{2.9}$$

$$= r \sum_{n\geq 0} r^n \frac{x^n}{n!} \tag{2.10}$$

$$= rE(x) \tag{2.11}$$

This is an easily solvable differential equation. We know that $E(x) = e^{rx}$ by elementary differential equations class. This means that $e^{rx} = \sum_{n\geq 0} \frac{r^n x^n}{n!}$. $\square$

3. Problem 3

Define a sequence B_n by the identity $f(x) := \frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$, i.e. B_n is $n!$ times the coefficient of x^n in the expansion of the left hand side, where one uses $e^x - 1 = \sum_{n=0}^{\infty} x^n/n!$.

Problem 3.1. *Calculate B_0 through B_{10}.*

Solution First, we can clearly see from the series expansion of the left hand side that $B_0 = 1$. Next, we see that if we multiply both sides of the definition of $f(x)$ by $(e^x - 1)$ and expand out the series, we obtain $x = (e^x - 1)\sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$. Using the fact that $\bar{A}(x)\bar{B}(x)$ generates the function $\{c_n\}$ where $c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$, we find:

$$x = \left(\sum_{n=0}^{\infty} (1) \frac{x^n}{n!}\right)\left(\sum_{n=0}^{\infty} B_n \frac{x^n}{n!}\right) \tag{3.1}$$

$$x = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k} B_k \tag{3.2}$$

Equating the coefficients of x^{n+1} on both sides of the expression, we find that:

$$0 = \sum_{k=0}^{n+1} \binom{n+1}{k} B_k \tag{3.3}$$

$$(n+1)B_n = -\sum_{k=0}^{n-1} \binom{n+1}{k} B_k \tag{3.4}$$

This means that we can use this recurrence to calculate $B_0, \ldots, B_{10}$. We obtain:

$$B_0 = 1 \tag{3.5}$$
$$B_1 = -\frac{1}{2} \tag{3.6}$$
$$B_2 = \frac{1}{6} \tag{3.7}$$
$$B_3 = 0 \tag{3.8}$$
$$B_4 = -\frac{1}{30} \tag{3.9}$$
$$B_5 = 0 \tag{3.10}$$
$$B_6 = \frac{1}{42} \tag{3.11}$$
$$B_7 = 0 \tag{3.12}$$
$$B_8 = -\frac{1}{30} \tag{3.13}$$
$$B_9 = 0 \tag{3.14}$$
$$B_{10} = \frac{55}{66} \tag{3.15}$$

□

Problem 3.2. *Show that for $n > 1$ odd, $B_n = 0$.*

Solution We see that $f(x) - f(-x)$ can be expanded into the following, using the series representations:

$$f(x) - f(-x) = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} - \sum_{n=0}^{\infty} B_n \frac{(-x)^n}{n!} \tag{3.16}$$
$$= \sum_{n \text{ odd}} B_n \frac{x^n}{n!} \tag{3.17}$$

Moreover, we know that $f(x) - f(-x)$ can also be represented as:

$$f(x) - f(-x) = \frac{x}{e^x - 1} - \frac{-x}{e^{-x} - 1} \tag{3.18}$$
$$= \frac{x(e^{-x} - 1) + x(e^x - 1)}{(e^x - 1)(e^{-x} - 1)} \tag{3.19}$$
$$= \frac{xe^{-x} + xe^x - 2x}{2 - e^x - e^{-x}} \tag{3.20}$$
$$= -x \tag{3.21}$$

Thus, equating these two expressions, we see that $B_1 = -1$, and that $B_n = 0$ for all odd n. □

Problem 3.3. *Establish the recurrence for $n \geq 2$ that $\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$.*

Solution We use the same method we used in part 1 and multiply both sides by $e^x - 1$. Thus, we find:

$$x = \left(\sum_{n=0}^{\infty} (1) \frac{x^n}{n!} \right) \left(\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} \right) \tag{3.22}$$
$$x = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k} B_k \tag{3.23}$$

Finding the coefficient of x^n on both sides, we see that $B_n = \sum_{k=0}^{n} \binom{n}{k} B_k$, which shows, since $\binom{n}{n} B_n = B_n$, that we have:

$$0 = \sum_{k=0}^{n-1} \binom{n}{k} B_k \tag{3.24}$$

This is what we wanted to show. □

Problem 3.4. *Let $S_k(n) = 1^k + 2^k + \ldots + n^k$ be the sum of the kth powers of the first n natural numbers. Show that S_k is given by the following polynomial of degree $k+1$ in n: $S_k(n) = \frac{1}{k+1} \sum_{i=0}^{k} (-1)^i \binom{k+1}{i} B_i n^{k+1-i}$.*

Solution First, we know that $\sum_{k\geq 0} S_k(n)\frac{x^k}{k!}$ can be computed as follows:

$$\sum_{k\geq 0} S_k(n)\frac{x^k}{k!} = \sum_{k=0}^{\infty}\left(\sum_{m=0}^{n} k^m\right)\frac{x^k}{k!} \tag{3.25}$$

$$= \sum_{m=0}^{n}\sum_{k=0}^{\infty}\frac{k^m x^k}{k!} \tag{3.26}$$

$$= \sum_{m=0}^{n} e^{mx} \tag{3.27}$$

Where the last line comes from the result we showed in problem 2. However, we know that $\sum_{m=0}^{\infty} e^{mx}$ is a geometric series which can be evaluted. We find:

$$\sum_{m=0}^{n} e^{mx} = \frac{e^{nx}-1}{e^x-1} \tag{3.28}$$

$$= \frac{e^{nx}-1}{x}\frac{x}{e^x-1} \tag{3.29}$$

$$= \left(\sum_{k=0}^{\infty}\frac{n^{k+1}}{k+1}\frac{x^k}{k!}\right)\left(\sum_{k=0}^{\infty} B_k\frac{x^k}{k!}\right) \tag{3.30}$$

And now we use result from problem 2 on the product of two exponential generating functions to continue this:

$$\sum_{k\geq 0} S_k(n)\frac{x^k}{k!} = \sum_{m=0}^{n} e^{mx} = \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k}\binom{k}{i}\frac{1}{k-i+1}B_i n^{k+1-i}\right)\frac{x^k}{k!} \tag{3.31}$$

Now, we can equate the coefficients of $\frac{x^k}{k!}$ on the left and right hand sides. We find:

$$S_k(n) = \sum_{i=0}^{k}\binom{k}{i}\frac{1}{k-i+1}B_i n^{k+1-i} \tag{3.32}$$

$$= \sum_{i=0}^{k}\frac{k!}{i!(k-i)!(k-i+1)}B_i n^{k+1-i} \tag{3.33}$$

$$= \sum_{i=0}^{k}\frac{1}{k+1}\binom{k+1}{i}B_i n^{k+1-i} \tag{3.34}$$

$$= \frac{1}{k+1}\sum_{i=0}^{k}(-1)^i\binom{k+1}{i}B_i n^{k+1-i} \tag{3.35}$$

Which is what we wanted to show. □

4. Problem 4

Problem 4.1. *Let m and n be two integers which are sums of two squares. Show that mn is a sum of two squares. Use this to show that any positive integer of the form $\prod p_i^{e_i}\prod q_j^{f_j}$, where p_i are primes which are 2 or 1 mod 4, and q_j are primes which are 3 mod 4, such that f_j are all even, is a sum of two integer squares.*

Solution First, if $m = a^2+b^2$ and $n = c^2+d^2$, then it is clear that mn is also a sum of two squares because we can write $mn = (a^2+b^2)(c^2+d^2) = (ac)^2+(ad)^2+(bc)^2+(bd)^2 = (ac+bd)^2+(ad-bc)^2$. This shows that mn is a sum of two squares.

Now, note that if p is a prime such that $p = 2$ or $p \equiv 1 \pmod 4$, then p is a sum of two squares by a theorem proven in class. This means that $\prod p_i^{e_i}$ is a sum of two squares, since $p_i^{e_i}$ are all sum of two squares and we can therefore apply our previous result.

Moreover, since q_j are all primes congruent to 3 (mod 4) where f_j are all even, we know that $q_j^{f_j} = (q_j^{f_j/2})^2+0^2$ is a sum of two squares. This, all of the q_j are sums of two squares, which means that $\prod q_j^{f_j}$ is a sum of two squares. Therefore, we see that $\prod p_i^{e_i}\prod q_j^{f_j}$ is a product of two squares given the assumptions of the problem. □

Problem 4.2. *Now suppose n is a sum of two integer squares. Show that it must have the form above, i.e. if a prime q which is 3 mod 4 divides n, then it must divide it to an even power.*

Solution We note that this is equivalent to proving that if q is a prime of the form 3 (mod 4), then it does not divide a sum of two coprime squares. Assume by contradiction that $q|x^2+y^2$ where $gcd(x,y)=1$. Thus, we see that $x^2+y^2 \equiv 0 \pmod{q}$. Since we can choose x and y mod q such that $-q/2 < x, y < q/2$, we can set $x^2+y^2 < (1/2)q^2$. Since we can write

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = \frac{x^2+y^2}{2} \tag{4.1}$$

We can substitute $a=(x+y)/2$ and $b=(x-y)/2$ and find that $qs = a^2+b^2$ where s is an odd number (since there are no factors of 2 left in a or b). Moreover, we know that $s<q$ since $x^2+y^2<(1/2)q^2$. Since a and b are coprime, $a^2+b^2 \equiv 1 \pmod{4}$. This means that $s \equiv 3 \pmod{4}$ so that s must have at least one prime factor $p \equiv 3 \pmod{4}$. Therefore, if $q \equiv 3 \pmod{4}$ divides a sum of two coprime squares, then $p \equiv 3 \pmod{4}$ less than q must also divide this sum of two coprime squares. However, we assumed that these squares were coprime, which is a contradiction. Therefore, $q \equiv 3 \pmod{4}$ must divide n to an even power if n is a sum of two integer squares. □

Problem 4.3. *Show that n is a sum of squares of two rational numbers if and only if it's a sum of squares of two integers.*

Solution It is clear that if n is a sum of squares of two integers, then it is also a sum of squares of two rational numbers. Thus, we only need to show that if n is a sum of square of two rational numbers, then it is a sum of squares of two integers. Now suppose $n=(a/b)^2+(c/d)^2$. We can rewrite this expression as $n(bd)^2=(ad)^2+(cb)^2$. Thus, we want to show that if there exist positive integers satisfying $m^2n=x^2+y^2$, then n can be written as a sum of squares of two integers.

Let t be choosen so that $t^2<n<(t+1)^2$. Since there are $(t+1)^2$ integers of the form $xu+yv$ where $0 \le u$ and $v \le t$, which is greater than n, we see that these numbers fill up a quadratic residue class modulo n. Thus, there are two numbers of the form $x(u-u')+y(v-v')$ which are divisible by n. We can set $w=u-u'$ and $z=v-v'$, knowing that $|w|,|z|<t$. This means that $n|x^2w^2-y^2z^2$. Moreover, we know that $n|x^2z^2+y^2z^2$. Therefore, n divides the sum of these two, so that $n|x^2(w^2+z^2)$. Since it is sufficient to show this when $gcd(x,n)=1$, we know that $n|w^2+z^2$. Since $x^2+y^2<2n$, we see that $n=w^2+y^2$. This completes the proof. □

5. Problem 5

Problem 5.1. *Let $\omega = e^{2\pi i/3}$ be a primitive cube root of unity. Write down the cyclotomic polynomial $\Phi_3(x)$ and thereby compute ω^2 in terms of ω. Now calculate the norm of the complex number $a+b\omega$. Use this to show that if m,n are two integers which can be written in the form a^2-ab+b^2, then their product can also be written likewise.*

Solution Using the factorization of x^3-1 for all factors x^k-1 where $k|3$, we find that $\Phi_3(x)=x^2+x+1$. Substituting $x=\omega$ into the polynomial, we find that $0=\omega^2+\omega+1$ so that $\omega^2=-\omega-1$. To find the norm of $a+b\omega$, we see that $(a+b\omega)(a+b\omega^2)=a^2+ab\omega^2+ab\omega+b^2\omega^3=a^2+ab(-1-\omega)+b^2=a^2-ab+b^2$. Thus, we see that $|a+b\omega|=a^2-ab+b^2$.

Now, we see that if an integer can be written in the form a^2-ab+b^2, then it is the norm of a complex number $a+b\omega$. Therefore, if two integers m,n can be written in the form a^2-ab+b^2, then they are the norms of two numbers $a+b\omega$. Now, we know that the product mn is the product of two norms. Since a product of two norms is also a norm, we know that mn can be written in the form a^2-ab+b^2. □

Problem 5.2. *Show that if p is a prime which can be written as a^2-ab+b^2, then p cannot be 2 (mod 3), so that $p=3$ or $p \equiv 1 \pmod{3}$.*

Solution If $p=a^2-ab+b^2$, then we can evaluate $a^2-ab+b^2 \equiv p \pmod{3}$. We shall see what p can be modulo 3. So we shall enumerate all the possibilities of $a,b \pmod{3}$ (i.e $a,b=\{0,1,2\}$) and observe what happens:

$$0^2-0*0+0^2 \equiv 0 \pmod{3} \qquad 0^2-0*1+1^2 \equiv 1 \pmod{3} \tag{5.1}$$

$$0^2-0*2+2^2 \equiv 1 \pmod{3} \qquad 1^2-0*0+0^2 \equiv 1 \pmod{3} \tag{5.2}$$

$$1^2-1*1+1^2 \equiv 1 \pmod{3} \qquad 1^2-1*2+2^2 \equiv 0 \pmod{3} \tag{5.3}$$

$$2^2-2*0+0^2 \equiv 1 \pmod{3} \qquad 2^2-2*1+1^2 \equiv 0 \pmod{3} \tag{5.4}$$

$$2^2-2*2+2^2 \equiv 1 \pmod{3} \tag{5.5}$$

Thus, for all combinations of $a, b \pmod 3$, it is impossible for $a^2 - ab + b^2$ to be equivalent to $2 \pmod 3$. This completes the theorem. □

6. Problem 6

Problem 6.1. *Show 3 and any prime p which is $1 \pmod 3$ can be written as $a^2 - ab + b^2$, for some integers a and b.*

Solution If $p = 3$ then $a = 2$ and $b = 1$ satisfies $p = 3 = a^2 - ab + b^2$. This means we can concern ourselves with all odd primes p such that $p \equiv 1 \pmod 3$. We shall use strong induction on the primes, so assume that every prime $q < p$ which is $1 \pmod 3$ can be written in the form $a^2 - ab + b^2$. Next, we will invoke the following lemma:

Lemma 6.1. *There exists a positive integer $m < p$ such that $a^2 - ab + b^2 = mp$.*

Proof. We know from a theorem proven earlier in class that if $f(x) = ax^2 + bx + c$, then the congruence $f(x) \equiv 0 \pmod p$ has one solution if $p \nmid 1$ and $p | b^2 - 4ac$. So let $f(x) = x^2 - bx + b^2$. We see that the congruence has a solution when $p | b^2 - 4b^2 = -3b^2$. Thus, the congruence has a solution when $p | 3b^2$. We can set $b = p$ so that this always occurs. Since this is the case, we see that $x = a$ and b can always be found such that $p | a^2 - ab + b^2$ so that $mp = a^2 - ab + b^2$. □

Now, if $m = 1$, then we are finished with the proof. If $m > 1$, we shall show that this results in a contradiction. So assume by contradiction that $m > 1$. We know that $a^2 - ab + b^2 < a^2 + b^2 < p^2$ because $m < p$. This implies that $|a| < p$ and $|b| < p$. We also know that $g = gcd(a, b) = 1$ because otherwise we could take $(a/g)^2 - (ab/g^2) + (b/g)^2 = (m/g^2)p$ and obtain a smaller m.

Next, we know that m must be odd. If not, then a^2, ab, b^2 must all be even (no other combination allows mp to be even. This implies that a and b must have the same parity. Therefore, we can set $A = (2a + b)/2$ and $B = (a + b)/2$ and obtain:

$$A^2 - AB + B^2 = \left(\frac{2a+b}{2}\right)^2 - \left(\frac{2a+b}{2}\frac{a+b}{2}\right) + \left(\frac{a+b}{2}\right)^2 \tag{6.2}$$

$$= \frac{3}{4}\left(a^2 - ab + b^2\right) \tag{6.3}$$

This contradicticts the minimality of m, so we see that m must be odd. Now, if we let q be an odd prime dividing m so that $m = qn$, we see that $a^2 - ab + b^2 = qnp$. We see that $q \nmid a$ and $q \nmid b$ or else q would divide both a and b which would contradict the fact that $gcd(a, b) = 1$. Moreover, we know that $a^2 - ab + b^2 \equiv 1 \pmod 3$ by the analysis given the previous problem. Thus, we see that $qpn \equiv 1 \pmod 3$. Since $p \equiv 1 \pmod 3$, we know that $qn \equiv 1 \pmod 3$. Since we have shown that $n \equiv 1 \pmod 3$ by the fact that n is odd, we must have $q \equiv 1 \pmod 3$.

Because of this, we can use the inductive hypothesis, so we know that $q = c^2 - cd + d^2$. Thus, if we multiply both sides of $a^2 - ab + b^2 = qpn$ by q, we obtain:

$$(a^2 - ab + b^2)(c^2 - cd + d^2) = pq^2n \tag{6.4}$$

Simplifying this expression, we find that $(ac - bd)^2 + (ad + bc)^2 - (ac - bd)(ad + bc) = pq^2n$. We see that $q | ac - bd$ and $q | ad + bc$ which implies:

$$\left(\frac{ac-bd}{q}\right)^2 + \left(\frac{ad+bc}{q}\right)^2 + \left(\frac{ac-bd}{q}\frac{ad+bc}{q}\right) = pn \tag{6.5}$$

However, since we know that $n < m$ since $qn = m$, we see that we have contradicted the minimality of m. This completes the proof. □

Problem 6.2. *An integer n can be written as $a^2 - ab + b^2$ if and only if $n > 0$ and every prime $p \equiv 2 \pmod 3$ which divides n, divides n to an even power.*

Solution In order to prove this theorem, we will invoke a lemma:

Lemma 6.6. *Let p be a prime equivalent to $2 \pmod 3$. Then no integer n divisible precisely by an odd power of p can be written in the form $a^2 - ab + b^2$.*

Proof. Let $p \equiv 2 \pmod 3$ and suppose by contradiction that $n = a^2 - ab + b^2$ where $p^{2s+1} || n$ for some integer s. Let $g = gcd(a, b)$ so that we can simplify the expression to the following: $n/g^2 = (a/g)^2 - (ab/g^2) + (b/g)^2$. Now, substitute $m = n/g^2$, $x = a/g$, and $y = b/g$ to obtain the expression

$$m = x^2 - xy + y^2, \qquad gcd(x, y) = 1 \tag{6.7}$$

We see that $p^{2s+1}||m$, which means that $x^2 - xy + y^2 \equiv 0 \pmod{p}$. Now we can choose A as an integer such that $2Ax = y \pmod{p}$. Substituting this expression for y, we find that $x^2 - x(2Ax) + (2Ax)^2 = x^2 - 2Ax^2 + 4A^2x^2 = x^2(4A^2 - 2A + 1) \equiv 0 \pmod{p}$. Completing the square and factorizing, this expression can be rewritten as $x^2 4^{-1}((4A-1)^2 + 3) \equiv 0 \pmod{p}$. However, we know that $p \nmid x$ because if it did, then $p|y^2$ because $m = x^2 + y^2 - xy$. This would imply that $p|y$, and clearly p does not divide both x and y. Therefore, we see that $(4A-1)^2 + 3 \equiv 0 \pmod{p}$.

Substituting $B = 4A - 1$, we find that $B^2 \equiv -3 \pmod{p}$. However, we know that $\left(\frac{-3}{p}\right) = -1$ because $p \equiv 2 \pmod{3}$. This is a contradiction because we have shown that $B^2 \equiv -3 \pmod{p}$. Therefore, we no integer n divisible by an odd power of p can be written in the form $a^2 - ab + b^2$ and we have completed the proof of the lemma. □

Now, let us go back to proving the original theorem and assume that n can be written as $a^2 - ab + b^2$. By the lemma, we see that all primes $p \equiv 2 \pmod{3}$ which divide n must have even powers when dividing n. This completes the first part of the proof.

For the converse, we let $n = p_1 p_2 \dots p_m q_1^{2e_1} \dots q_l^{2e_l}$ where $p_i \equiv 1 \pmod{3}$ and $q_i \equiv 2 \pmod{3}$. By part a of the problem, we see that p_i can be written as $a^2 - ab + b^2$ for some integers a and b. By a previous problem, we know that if n and m are integers that can be written in the form $a^2 - ab + b^2$, then their product can also be written in this form. This shows that the product $p_1 p_2 \dots p_m$ can be written in the form $a^2 - ab + b^2$. We also know that $q_i^{2e_i} = (q_i^{e_i})^2 - (0)q_i^{e_i} + 0^2$ can be written in the form $a^2 - ab + b^2$. Thus, we see that n, which is the product of a elements which can be written in the form $a^2 - ab + b^2$, can also be written in the form $a^2 - ab + b^2$. This completes the proof of the converse. □

7. Problem 7

Problem 7.1. *Calculate the continued fraction of* 6157/783.

Solution We first find that $6157/783 = 7 + 676/783$. Thus, the first digit of the continued fraction is 7. Next, we want to find the continued fraction of $\frac{783}{676}$. This comes out to $1 + \frac{107}{676}$. Thus, the second digit of the original continued fraction is 1. Performing the same operations, we obtain the following series of operations:

$$\frac{676}{107} = 6 + \frac{34}{107} \tag{7.1}$$

$$\frac{107}{34} = 3 + \frac{5}{34} \tag{7.2}$$

$$\frac{34}{5} = 6 + \frac{4}{5} \tag{7.3}$$

$$\frac{5}{4} = 1 + \frac{1}{4} \tag{7.4}$$

Thus, the continued fraction of 6157/783 comes out to $[7, 1, 6, 3, 6, 1, 4]$. □

Problem 7.2. *Calculate the continued fraction of* $\sqrt{15}$.

Solution The continued fraction of $\sqrt{15}$ can be calculated in the following manner, noting that $3 < \sqrt{15} < 4$:

$$\sqrt{15} = 3 + \frac{\sqrt{15} - 3}{1} = 3 + \frac{(\sqrt{15} - 3)(\sqrt{15} + 3)}{\sqrt{15} + 3} = 3 + \frac{6}{\sqrt{15} + 3} \tag{7.5}$$

$$= 3 + \frac{1}{\frac{\sqrt{15}+3}{6}} \tag{7.6}$$

Now, we shall compute the continued fraction of $\frac{\sqrt{15}+3}{6}$ to continue to find the continued fraction of $\sqrt{15}$:

$$\frac{\sqrt{15} + 3}{6} = 1 + \frac{\sqrt{15} - 3}{6} = 1 + \frac{(\sqrt{15} - 3)(\sqrt{15} + 3)}{6(\sqrt{15} + 3)} \tag{7.7}$$

$$= 3 + \frac{1}{\sqrt{15} + 3} \tag{7.8}$$

Proceeding onwards, we will find the continued fraction of $\sqrt{15}+3$:

$$\sqrt{15}+3 = 6+\frac{\sqrt{15}-3}{1} = 6+\frac{(\sqrt{15}-3)(\sqrt{15}+3)}{\sqrt{15}+3} = 6+\frac{6}{\sqrt{15}+3} \tag{7.9}$$

$$= 6+\frac{1}{\frac{\sqrt{15}+3}{6}} \tag{7.10}$$

We see that this has looped back to the continued fraction of $\frac{\sqrt{15}+3}{6}$. Therefore, we have found a recursive relationship, so that $\sqrt{15} = [3, 1, 6, 1, 6, \ldots]$. $\square$