18.781
PROBLEM SET 7

JOHN WANG

1. Problem 1

Problem 1.1. *Let S be a set of $n+1$ integers selected from $1, 2, \dots, 2n+1$. Prove that S contains two relatively prime integers. Show that the result doesn't hold if only n integers are chosen.*

Solution Suppose by contradiction that S does not contain two relatively prime integers. Then this means that some prime p divides all the integers in S. Thus, $p|s$ for all $s \in S$. This means that there must exist at least $n+1$ integers in the set which are divisible by p. However, we know that the smallest prime possible is 2, so that there can only possibly be $\lfloor 2n+1/2 \rfloor = n$ integers divisible by 2. This is a contradiction because one cannot pick $n+1$ distinct integers divisible by p from a set which contains at maximum only n integers divisible by p.

Now to show that the result doesn't hold for n integers, we take $n = 2$. From the set $1, 2, 3, 4, 5$, we shall pack $n = 2$ integers. We pick 2 and 4 which are not relatively prime. □

2. Problem 2

Problem 2.1. *Prove that among any ten consecutive positive integers there is at least one which is coprime to the product of the others.*

Solution Suppose not. Then there must be some common prime factor which divides each of the ten integers. However, we see that any common prime factor must be less than 10 because any common factor of x and y must also be a factor of $x - y$. This only leaves the primes 2,3,5, and 7 as possibilities to be common factors.

There will be five integers which are even in this set, and which will therefore be divisible by 2. These cannot be relatively prime to the rest. There can be at most two other integers which are divisible by 3. At most one other integer can be divisible by 5 (since the other integer divisible by 5 was taken into account by being even). Finally only one other integer can be divisible by 9. However, we see that there is no common factor which divides each of the ten integers, because there is one integer left which is not divisible by 2,3,5, or 7. This is a contradiction, so there must exist at least one integer which is coprime to the product of the others. □

3. Problem 3

Problem 3.1. *At a party, there are n people, who each give their coat to a coat-check person. Calculate the number of ways in which the coats can be handed back, each person receiving one, so that no one receives their own coat.*

Solution Let $f(n)$ be the number of ways in which n coats can be handed back so no one receives their own coat. Label all of the people and theirs coats from $1, \dots, n$. Now, person 1 could be given person i's coat, and there are $n-1$ ways to choose i. Once this has occurred, then person i can either get coat 1 or not get coat 1. If he gets coat 1, then there are $n-2$ coats and $n-2$ people, so there are $f(n-2)$ ways for the coats to be handed back in this case. In the other case, person i does not get coat 1, so that there are $n-1$ possibilities of coats to choose from (anything by coat 1). There are $f(n-1)$ ways to distribute the rest of the coats in this case. This gives the recurrence:

$$f(n) = (n-1)(f(n-2) + f(n-1)) \tag{3.1}$$

We know that in the base case, $f(1) = 0$ because there is only one way to hand the coats back with 1 person, and it will always be to the correct person. Also, $f(0) = 1$ because when there is nobody there,

there is one way to make no on receive their own coat. Now subtract $nf(n-1)$ from both sides of the above expression:

$$f(n) - nf(n-1) = -(f(n-1) - (n-1)f(n-2)) \tag{3.2}$$
$$f(n) - nf(n-1) = (-1)^n \tag{3.3}$$

Because of the fact that $f(1) = 0$ and $f(0) = 1$ so that $f(2) - 2f(1) = -(f(1) - (2-1)f(0)) = 1$, which implies that $f(3) - 3f(2) = -1$. Clearly, this is just an alternating of 1 and -1. Now, we find the following:

$$\frac{f(n)}{n!} - \frac{f(n-1)}{(n-1)!} = \frac{(-1)^n}{n!} \tag{3.4}$$
$$\frac{f(n)}{n!} = \frac{(-1)^n}{n!} + \frac{f(n-1)}{(n-1)!} \tag{3.5}$$
$$= \frac{(-1)^n}{n!} + \frac{(-1)^{n-1}}{(n-1)!} + \ldots + \frac{(-1)^0}{0!} \tag{3.6}$$
$$= \sum_{i=0}^{n} \frac{(-1)^i}{i!} \tag{3.7}$$

Therefore, we find the following expression for $f(n)$:

$$f(n) = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!} \tag{3.8}$$

□

4. Problem 4

Problem 4.1. *Prove that $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$ for any positive integers m and n. Then prove that $F_m | F_n$ if $m|n$.*

Solution We will prove this by induction. First assume that this holds for some m and two consecutive values of n. Then we know that

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1} \tag{4.1}$$
$$F_{m+(n-1)} = F_{m-1}F_{n-1} + F_mF_n \tag{4.2}$$

Therefore, using the fibonacci recurence, we find the following:

$$F_{m+(n+1)} = F_{m+n} + F_{m+n-1} \tag{4.3}$$
$$= F_{m-1}F_n + F_mF_{n+1} + F_{m-1}F_{n-1} + F_mF_n \tag{4.4}$$
$$= F_{m-1}(F_n + F_{n-1}) + F_m(F_{n+1} + F_n) \tag{4.5}$$
$$= F_{m-1}F_{n+1} + F_mF_{n+2} \tag{4.6}$$

Which is what we wanted to show on the induction step. Now assume that this holds for some n and two consecutive values of m. Then we can write down:

$$F_{(m-1)+n} = F_{m-2}F_n + F_{m-1}F_{n+1} \tag{4.7}$$

Substituting this into the fibonacci recurrence, we get:

$$F_{(m+1)+n} = F_{m+n} + F_{m-1+n} \tag{4.8}$$
$$= F_{m-1}F_n + F_mF_{n+1} + F_{m-2}F_n + F_{m-1}F_{n+1} \tag{4.9}$$
$$= (F_{m-1} + F_{m-2})F_n + (F_m + F_{m-1})F_{n+1} \tag{4.10}$$
$$= F_mF_n + F_{m+1}F_{n+1} \tag{4.11}$$

Which is what we wanted to show. Since the induction works for both m and n fixed, the formula has been proven. □

5. Problem 5

Let $r(n)$ be the number of ways of writing a positive integer n in the form $n = m_1 + m_2 + \ldots + m_k$ where k and $m_1, \ldots, m_k$ are arbitrary positive integers.

Problem 5.1. *Show that $r(n) = 1 + r(1) + r(2) + \ldots + r(n-1)$ for $n \geq 2$. Deduce that $r(n) = 2r(n-1)$ for $n \geq 2$ and therefore that $r(n) = 2^{n-1}$ for all positive integers n.*

Solution Clearly $r(0) = 1$ because there is only one way to write $0 = m_1+m_2+\ldots+m_k$ where $m_1, \ldots, m_k$ are arbitrary positive integers, and also $r(1) = 1$. Now let us find $r(n)$. We know that the number of ways to sum up to n is just the number of ways to sum up to $n-i$ plus the number of ways to sum up to i for all $i \in \{1, 2, \ldots, n/2\}$ plus 1 for $0 + n$. Thus, we find that:

$$r(n) = 1 + \sum_{i=1}^{n/2} r(n-i) + r(i) = 1 + r(1) + r(2) + \ldots + r(n-1) \tag{5.1}$$

We shall show that $r(n) = 2r(n-1)$ by induction. This clearly holds for $r(2) = 2 = 2r(1)$. Now suppose it holds up to n. Then we know that $r(n+1) = 1+r(1)+r(2)+\ldots+r(n) = (1+r(1)+r(2)+\ldots+r(n-1))+r(n) = r(n) + r(n) = 2r(n)$. Therefore, we see that $r(n) = 2r(n-1)$ holds for all $n \geq 2$. Now we can solve this congruence using the characteristic polynomial:

$$r(n) - 2r(n-1) = 0 \tag{5.2}$$
$$\lambda - 2 = 0 \tag{5.3}$$

Therefore, we find that $r(n) = \alpha 2^n$. Since we know that $r(1) = 1$, we see that $r(1) = 1 = 2^1\alpha$ so that $\alpha = 1/2$. Therefore, we see that $r(n) = 2^{n-1}$. □

Problem 5.2. *Establish this formula for $r(n)$ directly by a combinatorial argument.*

Solution We know that the number of ways to sum up to n using k different positive integers is $\binom{n-1}{k-1}$. This is because one can enumerate n with n different objects representing 1. Then, there are $n-1$ different places you can pick to divide up the objects. Moreover, you have $k-1$ different dividing places to use in order to obtain a total of k different groups. This means you have $\binom{n-1}{k-1}$ ways of summing to n using k different positive integers. Therefore, we find that $r(n)$ can be expressed as a sum over all feasible k:

$$r(n) = \sum_{k=1}^{n} \binom{n-1}{k-1} \tag{5.4}$$
$$= \sum_{i=0}^{n-1} \binom{n-1}{i} \tag{5.5}$$

This is just the sum of all the binomial coefficients of $n-1$. By a well known theorem, we know that this is equal to 2^{n-1}. This completes the combinatorial proof. □

6. Problem 6

Problem 6.1. *Show that the number of ways of writing a positive integer n in the form $n = m_1+m_2+\ldots+m_k$ where k is an arbitrary positive integer and $m_1, \ldots, m_k$ are arbitrary odd positive integers is F_n.*

Solution First denote $o(n)$ as the number of ways to write n in the form $n = m_1 + \ldots + m_k$ where $m_1, \ldots, m_k$ are arbitrary odd positive integers. We see that $o(n) = o(1) + o(3) + o(5) + \ldots + o(n-1)$. This is because the number of ways to sum up to n using odd integers is the number of ways to sum to $n-i$ plus the number of ways to sum to i where $n-i$ and i are odd for all $i \in \{1, 2, \ldots, n/2\}$. This means we have $o(n) = 1 + \sum_{i=1}^{n/2} o(n-i) + o(i) = 1 + o(3) + \ldots + o(n-1)$.

Now we shall show that $o(n) = o(n-1)+o(n-2)$ by induction. We know trivially that $o(2) = 1, o(1) = 1$, and $o(0) = 0$. Therefore it holds for the base case of $n = 2$. Now, suppose it holds up to n. Then we know that $o(n+1) = o(1) + o(3) + \ldots + o(n-2) + o(n) = (o(1) + o(3) + \ldots + o(n-2)) + o(n) = o(n-1) + o(n)$. Therefore, we find that $o(n) = o(n-1) + o(n-2)$. Since $F_n = F_{n-1} + F_{n-2}$ and $F_0 = 0, F_1 = 1, F_2 = 1$, we see that $o(n)$ and F_n have the exact same recurrence and base cases. Therefore, we see that $o(n) = F_n$ which is what we wanted to show. □

7. Problem 7

Problem 7.1. *Let $f(n)$ be the number of sequences $a_1, \ldots, a_n$ which can be constructed with each $a_i \in \{0,1,2\}$ and such that the sequence cannot contain two consecutives 0s or two consecutive 1s. Prove that $f(n)$ is the integer closest to $\frac{1}{2}(1+\sqrt{2})^{n+1}$.*

Solution First we see that for a sequence of length n, we can have any valid a sequence of length $n-1$ without any consecutive 0s or 1s, and append a 2 at the end of the sequence. There are $f(n-1)$ of these sequences. Otherwise, we could have a sequence of k digits, alternating between 0 and 1, then a 2, and finally a sequence of length $n-k-1$ which contains no consecutive 0s or 1s. There are two ways to have a sequence of k digits alternating between 0 and 1, and there are $f(n-k-1)$ sequences of length $n-k-1)$ without consecutive 0s or 1s. This holds for all k such that $0 \le k \le n-1$. This means we have the following recurrence:

$$f(n) = f(n-1) + 2f(n-2) + 2f(n-3) + \ldots + 2 \tag{7.1}$$

We will show by induction that $f(n) = 2f(n-1) + f(n-2)$. Assume that this is true up to n. We shall show it is true to $n+1$. We see that this means that $2f(n-1) = f(n) - f(n-2)$. This implies

$$f(n+1) = f(n) + 2f(n-1) + 2f(n-2) + \ldots + 2 \tag{7.2}$$

$$= f(n) + (f(n) - f(n-2)) + (f(n-1) - f(n-3)) + \ldots + f(0) \tag{7.3}$$

$$= 2f(n) + f(n-1) \tag{7.4}$$

Where the second equation is a telescoping sum. We wanted to show that $f(n+1) = 2f(n) + f(n-1)$, and so we have concluded the induction step. Therefore, we can solve the recurrence $f(n) = 2f(n-1) + f(n-2)$, and we find the characteristic polynomial is $x^2 - 2x - x = 0$. The roots of this polynomial are $x = 1 \pm \sqrt{2}$. Since we know $f(0) = 1$ and $f(1) = 3$, we can solve for the terms α, β in the system:

$$f(n) = \alpha(1+\sqrt{2})^n + \beta(1-\sqrt{2})^n \tag{7.5}$$

Solving for initial conditions shows us that $\alpha = (2+\sqrt{2})/(2\sqrt{2})$ and $\beta = 1/2 - 1/\sqrt{2}$. We see that $|1-\sqrt{2}| < 1$ and that $|1+\sqrt{2}| > 1$. Because of this, we see that the term $\beta(1-\sqrt{2})^n \to 0$ as $n \to \infty$. Thus, we see that $f(n)$ converges to the integer nearest to $\alpha(1+\sqrt{2})^n$. This means that $f(n)$ will be the integer closest to $\frac{1}{2}(1+\sqrt{2})^{n+1}$ because $\alpha > 1 + \sqrt{2}$. □

8. Problem 8

Problem 8.1. *Let $p > 5$ be a prime. Show that $F_p \equiv \binom{p}{5} \pmod{p}$. Show that $F_{p+1} \equiv 1 \pmod{p}$ if $p \equiv \pm 1 \pmod{5}$ and $F_{p+1} \equiv 0 \pmod{p}$ if $p \equiv \pm 2 \pmod{5}$. Conclude that if $p \equiv \pm 1 \pmod{5}$, then $p-1$ is a period of the sequence $F_n \pmod{p}$.*

Solution We know that $F_p = \frac{1}{\sqrt{5}}\left(((1+\sqrt{5})/2)^p - ((1-\sqrt{5})/2)^p\right)$. Using the binomial formula, we can expand this out and cancel out terms to obtain:

$$F_p = \frac{1}{2^{p-1}\sqrt{5}}\left(1 + \binom{p}{1}\sqrt{5} + \ldots + \binom{p}{p}\sqrt{5}^p - \left(1 - \binom{p}{1}\sqrt{5} + \ldots + \binom{p}{2}\sqrt{5}^p\right)\right) \tag{8.1}$$

$$= \frac{1}{2^{p-1}\sqrt{5}}\left(\binom{p}{1}\sqrt{5} + \binom{p}{3}\sqrt{5}^2 + \ldots + \binom{p}{p}\sqrt{5}^p\right) \tag{8.2}$$

$$= \frac{1}{2^{p-1}}\left(\binom{p}{1}1 + \binom{p}{3}\sqrt{5} + \ldots + \binom{p}{p}\sqrt{5}^{p-1}\right) \tag{8.3}$$

Now we know that for $k = 1, 3, \ldots, p-1$ we have $\binom{p}{k} \equiv 0 \pmod{p}$. Therefore, we find that all of the terms are zero except the last one and we find $F_p \equiv \frac{1}{2^{p-1}}\binom{p}{p}\sqrt{5}^{p-1} \pmod{p}$. This means that $F_p \equiv 5^{(p-1)/2} \pmod{p}$ (since $2^{p-1} \equiv 1 \pmod{p}$ by Fermat) which shows $F_p \equiv \binom{p}{5} \pmod{p}$.

Now we show that $F_{p+1} \equiv 1 \pmod{p}$ if $p \equiv \pm 1 \pmod{5}$ and $F_{p+1} \equiv 0$ if $p \equiv \pm 2 \pmod{5}$. We know that $F_{p+1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^p + \left(\frac{1-\sqrt{5}}{2}\right)^p\right)$. We use the binomial expansion again and cancel terms to obtain:

$$F_{p+1} = \frac{1}{2^p}\left(\binom{p+1}{1}5^0 + \binom{p+1}{3}5^1 + \ldots + \binom{p+1}{p}5^{(p-1)/2}\right) \tag{8.4}$$

$$\equiv 1 + 5^{(p-1)/2} \pmod{p} \tag{8.5}$$

We arrive at this using the same arguments as above, and the fact that $\binom{p+1}{1} = \binom{p+1}{p} \equiv 1 \pmod{p}$. Since we know that $5^{(p-1)/2} \equiv \binom{5}{p} \equiv F_p \pmod{p}$, we can write that $2^p F_{p+1} \equiv 1 + F_p \pmod{p}$. Since $2^{p-1} \equiv 1$

(mod p) by Fermat, we see that $2F_{p+1} \equiv 1 + F_p \pmod{p}$. Thus if $F_p \equiv 1 \pmod{p}$ then $F_{P+1} \equiv 1 \pmod{p}$. Otherwise, if $F_p \equiv -1 \pmod{p}$, then $F_{p+1} \equiv 0 \pmod{p}$. Moreover, we know that $\left(\frac{5}{p}\right) = 1$ when $p \equiv \pm 1 \pmod{5}$ and $\left(\frac{5}{p}\right) = -1$ when $p \equiv \pm 2 \pmod{5}$. This is exactly what we wanted to show, since $F_p \equiv \left(\frac{5}{p}\right) \pmod{p}$.

Now, we move on to show that if $p \equiv \pm 1 \pmod{5}$, then $p - 1$ is a period of the sequence $F_n \pmod{p}$. First, we know that if $p \equiv \pm 1 \pmod{5}$, then $F_{p+1} \equiv 1 \pmod{p}$. We want to show that $p|F_{p+n-1} - F_n$ for arbitrary $n \in$ N. In otherwords, we shall show that $F_{p+n-1} \equiv F_n \pmod{p}$. If $n = 1$, we know that $F_p \equiv \left(\frac{5}{p}\right) \equiv F_1 \equiv 1 \pmod{p}$. This follows because $\left(\frac{5}{p}\right) = 1$ when $p \equiv \pm 1 \pmod{5}$. Now suppose this holds up to n. We shall show that it also holds for $n + 1$. We must evaluate the following:

$$\begin{aligned}
F_{p+(n+1)-1} &\equiv F_{p+n} \pmod{p} &(8.6)\\
&= F_{p+n-1} + F_{p+n-2} \pmod{p} &(8.7)\\
&= F_n + F_{n-1} \pmod{p} &(8.8)\\
&= F_{n+1} \pmod{p} &(8.9)
\end{aligned}$$

Where we have used the fact that $F_{p+n} = F_{p+n-1} + F_{p+n-2}$ and the induction hypothesis on $F_{p+n-1} \equiv F_n \pmod{p}$ and $F_{p+n-2} \equiv F_{n-1} \pmod{p}$. Since we see that $F_{p+(n+1)-1} \equiv F_{n+1} \pmod{p}$, we are done with the induction and have proven that $p - 1$ is a period of the sequence $F_n \pmod{p}$. □