18.781 Solutions to Problem Set 7

1. If the number 1 is in S, we're done since it's relatively prime to everything. So suppose $1 \notin S$. Break up the remaining elements into n pairs $\{2,3\}, \{4,5\}, \ldots, \{2n, 2n+1\}$. By the Pigeonhole Principle, since S contains $n+1$ elements, it has to have two elements from some pair. These two numbers are consecutive, and thus coprime.

   If only n elements are chosen, the result doesn't hold, because we can choose the even elements.

2. Let $S = \{n, \ldots, n+9\}$ be the set of 10 consecutive positive integers. If some prime p divides two elements of the set, then it divides the difference of them, so it divides some natural number between 1 and 9 (inclusive). So the only possibilities for p are 2, 3, 5, 7. Now we'll call $x \in S$ "bad" if it's not coprime to everything else in S, and good if it is. The strategy is to show that there are at most 9 bad elements of S, so there must be at least one good element, using an inclusion-exclusion argument.

   By the above reasoning, if x is bad, it has to be divisible by 2, 3, 5, or 7. Now there are exactly five elements of S divisible by 2, so we put these in the "bad" set. There are either four or three elements of S divisible by 3 (depending on whether n is divisible by 3 or not). But correspondingly, either two or one of these elements will be divisible by 6, and hence already in the bad set. So we add two new elements to the bad set. Then there are exactly two elements of S divisible by 5, but one of them is divisible by 10, so we can only add one extra bad element. Finally, there's exactly one element of S divisible by 7, and it might or might not be in the bad set already. This leaves us with at most nine elements in the bad set. Therefore, there exists a good element of S.

3. The total number of possible ways to hand back the coats is $n!$. Now, the number of ways to hand back the coats so that person i definitely gets back their own coat is $(n-1)!$. The number of ways to hand back the coats so that persons i and j both get back their coat is $(n-2)!$, and so on. So by inclusion-exclusion, the total number of ways no one gets back their own coat is

$$n! - n(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \cdots + (-1)^n \binom{n}{n}(n-n)!,$$

   which can be re-written as

$$n! \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!} \right).$$

   Note that if n is very large, this expression is approximately $n!/e$. So the probability that no one receives their coat back is approximately $1/e \approx 36.79\%$.

4. One can try to prove this relation by induction, but it's easier using the explicit formula $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$,

where $\alpha > \beta$ are the roots of $x^2 - x - 1 = 0$. Noting that $\alpha\beta = -1$, we have

$$\begin{aligned}
F_{m-1}F_n + F_mF_{n+1} &= \left(\frac{\alpha^{m-1} - \beta^{m-1}}{\alpha - \beta}\right)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) + \left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)\left(\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}\right) \\
&= \frac{1}{(\alpha - \beta)^2}\left[\alpha^{m+n-1} + \beta^{m+n-1} - \alpha^{m-1}\beta^n - \beta^{m-1}\alpha^n\right. \\
&\qquad\qquad \left. + \alpha^{m+n+1} + \beta^{m+n+1} - \alpha^m\beta^{n+1} - \beta^m\alpha^{n+1}\right] \\
&= \frac{1}{(\alpha - \beta)^2}\left[\alpha^{m+n+1} + \beta^{m+n+1} + \alpha^{m+n-1} + \beta^{m+n-1}\right] \\
&= \frac{1}{(\alpha - \beta)^2}\left[\alpha^{m+n+1} + \beta^{m+n+1} - \alpha^{m+n}\beta - \beta^{m+n}\alpha\right] \\
&= \frac{1}{(\alpha - \beta)^2}(\alpha^{m+n} - \beta^{m+n})(\alpha - \beta) \\
&= F_{m+n}.
\end{aligned}$$

Next, we need to show $F_m \mid F_n$ if $m \mid n$. Let's do this by induction on k, where $n = mk$. For $k = 0$ this is clear since $F_0 = 0$ is divisible by F_m. Now suppose the inductive hypothesis is true for $k - 1$. In the expansion

$$F_{mk} = F_{m(k-1)+m} = F_{m(k-1)-1}F_m + F_{m(k-1)}F_{m+1},$$

the terms F_m and $F_{m(k-1)}$ are both divisible by F_m, so F_{mk} is divisible by F_m, completing the induction.

5. (a) We want to show that $r(n) = 1 + r(1) + \cdots + r(n-1)$. If $m_1 = n$ then the decomposition is just $n = n$. If $m_1 = 1$, then the number of decompositions is the number of ways to choose $m_2, \ldots, m_k$ such that $n-1 = m_2 + \cdots + m_k$, which is $r(n-1)$. Similarly, if $m_1 = 2$, there are $r(n-2)$ decompositions, and so on. So $r(n) = 1 + r(1) + \cdots + r(n-1)$. Now since $r(n-1) = 1 + r(1) + \cdots + r(n-2)$, we see that $r(n) = (1 + r(1) + \cdots + r(n-2)) + r(n-1) = 2r(n-1)$. By induction on n, with the base case $r(1) = 1$, we must have $r(n) = 2^{n-1}$.

   (b) Note that for $n = m_1 + \cdots + m_k$, we must have $k \leq n$. Now consider n pebbles in a row, between which there are $n-1$ spaces. For each space we can either choose to place a bar there or leave an empty space. Each such set of choices bijectively corresponds to a decomposition of n. It follows that there are exactly 2^{n-1} choices.

6. Let $f(n)$ be the number of odd decompositions. Then, as in part (a) of the previous problem,

$$f(n) = \begin{cases} f(n-1) + f(n-3) + \cdots + f(1) & \text{if } n \text{ is even} \\ f(n-1) + f(n-3) + \cdots + f(2) & \text{if } n \text{ is odd.} \end{cases}$$

   The recurrence $f(n) = f(n-1) + f(n-2)$ follows immediately. Since $f(1) = 1 = F_1$ and $f(2) = 1 = F_2$, we must have $f(n) = F_n$ for all n.

7. Let $f(n)$ be the number of all such sequences, and let $g(n)$ be the number of such sequences which start with 0. Then, by symmetry, $g(n)$ is also equal to the number of such sequences starting with 1. When a sequence starts with 2, there are no further restrictions. So by considering the first element of the sequence, we get the recurrence

$$f(n) = g(n) + g(n) + f(n-1).$$

   By considering the second element of the sequence when the first element is 0, we get

$$g(n) = g(n-1) + f(n-2).$$

   Substituting from the first equation,

$$\frac{f(n) - f(n-1)}{2} = \frac{f(n-1) + f(n-2)}{2} + f(n-2),$$

which when rearranged becomes

$$f(n) - 2f(n-1) - f(n-2) = 0.$$

The characteristic polynomial has roots $1 \pm \sqrt{2}$, so $f(n) = A(1+\sqrt{2})^n + B(1-\sqrt{2})^n$. We can easily calculate $f(1) = 3, f(2) = 7$ to solve for A and B, obtaining

$$f(n) = \frac{1}{2}(1+\sqrt{2})^{n+1} + \frac{1}{2}(1-\sqrt{2})^{n+1}.$$

Since $-1 < 1-\sqrt{2} < 0$, $f(n)$ must be the integer closest to $\frac{1}{2}(1+\sqrt{2})^{n+1}$.

8. Using the explicit formula for F_n,

$$\begin{aligned} F_p &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^p - \left(\frac{1-\sqrt{5}}{2}\right)^p\right) \\ &= \frac{1}{2^{p-1}}\left[\binom{p}{1} + \binom{p}{3}5 + \binom{p}{5}5^2 + \cdots + \binom{p}{p-2}5^{\frac{p-3}{2}} + \binom{p}{p}5^{\frac{p-1}{2}}\right]. \end{aligned}$$

Reducing mod p and noting that $\binom{p}{1}, \ldots, \binom{p}{p-2}$ are all divisible by p, we get

$$F_p \equiv \frac{1}{2^{p-1}} \cdot 5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right) \pmod{p},$$

using Fermat's Little Theorem and Euler's criterion. By quadratic reciprocity, $(\frac{5}{p}) = (\frac{p}{5})$, so $F_p \equiv (\frac{p}{5}) \pmod{p}$. Therefore,

$$F_p \equiv \begin{cases} 1 \pmod{p} & \text{if } p \equiv \pm 1 \pmod{5} \\ -1 \pmod{p} & \text{if } p \equiv \pm 2 \pmod{5}. \end{cases}$$

Now let's compute

$$F_{p+1} = \frac{1}{2^p}\left[\binom{p+1}{1} + \binom{p+1}{3}5 + \cdots + \binom{p+1}{p}5^{\frac{p-1}{2}}\right].$$

Note that $\binom{p+1}{1} = \binom{p+1}{p} \equiv 1 \pmod{p}$, but $\binom{p+1}{3}, \ldots, \binom{p+1}{p-2}$ are all divisible by p. One way to see this is to use the rule

$$\binom{a_r p^r + \cdots + a_0}{b_r p^r + \cdots + b_0} \equiv \binom{a_r}{b_r} \cdots \binom{a_0}{b_0} \pmod{p}.$$

Now, using Fermat's Little Theorem,

$$F_{p+1} \equiv \frac{1}{2}(1 + 5^{\frac{p-1}{2}}) \pmod{p}.$$

When $p \equiv \pm 1 \pmod{5}$, $(\frac{5}{p}) = 1$ and thus $F_{p+1} \equiv 1 \pmod{p}$. When $p \equiv \pm 2 \pmod{5}$, $(\frac{5}{p}) = -1$ and thus $F_{p+1} \equiv 0 \pmod{p}$.

Finally, if $p \equiv \pm 1 \pmod{5}$, then $F_{p-1} = F_{p+1} - F_p \equiv 0 \pmod{p}$, so by Problem 4,

$$\begin{aligned} F_{n+p-1} &= F_{n-1}F_{p-1} + F_n F_p \\ &\equiv F_{n-1} \cdot 0 + F_n \cdot 1 \\ &\equiv F_n \pmod{p}. \end{aligned}$$

Therefore, $p-1$ is a period.

9. (a) The subset $\{n+1, \ldots, 2n\}$ has size n and property P.
   Now if S has size $n+1$ then consider the odd part of every element of S (if $x = 2^k y$ with y odd, then y is the odd part of x). There are n possible odd parts (namely $1, 3, \ldots, 2n-1$) and $n+1$ integers in S. Therefore, two elements must have the same odd part. So we have $x, x' \in S$ with $x = 2^k y$ and $x' = 2^l y$. Since either $k < l$ or $k > l$, one of x, x' must divide the other.

(b) The same proof shows that no subset of $n+1$ elements can have property P. As for a subset of n elements with property P, the subset $\{n, n+1, \ldots, 2n-1\}$ works.

(c) As in part (a), we write each element in the form $x = 3^k y$, where y is relatively prime to 3. Now there are $\lfloor (2n+2)/6 \rfloor$ multiples of 3 in the set $\{1, 3, 5, \ldots, 2n-1\}$, so there are $n - \lfloor (n+1)/3 \rfloor$ possible choices for y, setting an upper bound for the size of S. To show this bound is attainable, we form S by omitting elements $1, 3, 5, \ldots, 2\lfloor (n+1)/3 \rfloor - 1$. Since

$$3\left(2\left\lfloor \frac{n+1}{3} \right\rfloor + 1\right) \geq 3\left(2 \cdot \frac{n-1}{3} + 1\right) > 2n-1,$$

no two elements of S can divide each other.

10. (a) Consider any parenthesization of $x_0 \cdots x_{n+1}$. The left-most symbol in the expression is either "(" or x_0. If it's x_0 then the expression is $x_0 \cdot$ (some parenthesization of the product $x_1 \cdots x_{n+1}$), and the number of ways this can occur is C_n. If the left-most symbol is "(" then the ")" which pairs with it falls after x_i for some $i \geq 1$, and we must have (some parenthesization of $x_0 \cdots x_i$) $\cdot$ (some parenthesization of $x_{i+1} \cdots x_{n+1}$). The number of ways that this can occur is $C_i C_{n-i}$. So

$$C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}.$$

(b) The coefficient of z^n in $zC(z)^2$ is the coefficient of z^{n-1} in $C(z)^2$, which is equal to $C_0 C_{n-1} + C_1 C_{n-2} + \cdots + C_{n-1} C_0 = C_n$. To match up when $n = 0$, we add 1. So $C(z) = 1 + zC(z)^2$.

(c) Solving the quadratic equation $zC(z)^2 - C(z) + 1 = 0$, we get

$$C(z) = \frac{1 \pm \sqrt{1-4z}}{2z}.$$

Now $C(z)$ is a polynomial in z, so the minus sign must be taken in order to cancel out the constant term in the numerator. Now the coefficient of z^n in $C(z)$ is half the coefficient of z^{n+1} in $1 - (1-4z)^{1/2}$:

$$\begin{aligned}
[z^n]\, C(z) &= -\frac{1}{2}\binom{1/2}{n+1}(-4)^{n+1} \\
&= -\frac{1}{2}\frac{\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\cdots\left(\frac{1}{2}-n\right)}{(n+1)!}(-4)^{n+1} \\
&= \frac{(-1)^{n+1}}{2^{n+2}}\frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{(n+1)!}(-1)^{n+1}4^{n+1} \\
&= 2^n \frac{1 \cdot 2 \cdot 3 \cdots 2n}{(n+1)!(2 \cdot 4 \cdot 6 \cdots 2n)} \\
&= 2^n \frac{(2n)!}{(n+1)! 2^n n!} \\
&= \frac{1}{n+1}\binom{2n}{n}.
\end{aligned}$$

18.781 Theory of Numbers
Spring 2012