21-127 Concepts Homework 8: Solutions

6.2 All natural numbers except for multiples of p are coprime to p prime.

6.8 a) We apply the Euclidean algorithm,

$$\begin{aligned} 224 &= 126 + 98 \\ 126 &= 98 + 28 \\ 98 &= 3.28 + 14 \\ 28 &= 2.14 + 0 \end{aligned}$$

so the HCF is 14.

b) similarly,

$$\begin{aligned} 299 &= 221 + 78 \\ 221 &= 2.78 + 65 \\ 78 &= 65 + 13 \\ 65 &= 5.13 + 0 \end{aligned}$$

so the HCF is 13.

6.9 a) Applying the Euclidean algorithm,

$$\begin{aligned} 17 &= 13 + 4 \\ 13 &= 3.4 + 1 \end{aligned}$$

Working backwards we see $1 = 13 - 3.4 = 13 - 3(17 - 13) = 4.13 - 3.17$ so $200 = 800.13 - 600.17$ giving $x = -600$, $y = 800$ as a solution.

b) Likewise,

$$\begin{aligned} 21 &= 15 + 6 \\ 15 &= 2.6 + 3 \\ 6 &= 2.3 + 0 \end{aligned}$$

again working backwards,

$$\begin{aligned} 3 &= 15 - 2.6 \\ &= 15 - 2.(21 - 15) \\ &= 3.15 - 2.21 \\ \Rightarrow 93 &= 93.15 - 62.21 \end{aligned}$$

giving solution $x = -62$, $y = 93$.

6.23 Note that at least one of n, $n+2$, $n+4$ must be divisible by 3. (This can be seen either by considering the three possibilities $n = 3k$, $n = 3k+1$, $n = 3k+2$ for some $k \in \mathbb{Z}$ or more quickly by observing that each of the three numbers is in a different congruence class mod 3). They are prime, so one of them must actually be equal to 3, and the only possibility for this is $n = 3$.

6.40 $2^n - 1$ is prime, so the factors of $2^{n-1}(2^n - 1)$ are $\{1, 2, ..., 2^{n-1}, (2^n - 1), 2(2^n - 1), ..., 2^n(2^n - 1)\}$. The sum of these is $(1+2+...+2^{n-1})(1+(2^n - 1)) = (2^n-1)2^n$. If we exclude $2^{n-1}(2^n-1)$ itself then the sum is $(2^n-1)2^{n-1}$.

7.11 a) This is not an equivlence relation as it is not transitive. For example $2R6$ and $6R3$ but not $2R3$.

b) This is an equivalence relation:
Reflexive: for any $x \in \mathbb{R}$ we have $x = 2^0 x$.
Symmetric: given $x = 2^n y$ then $y = 2^{-n} x$
Transitive: given $x = 2^n y$ and $y = 2^m z$ then $x = 2^{n+m} z$

7.15 This assumes that for any $x \in S$ there is some $y \in S$ such that $(x, y) \in R$ but this may not in fact be true. (If it is then it is indeed the case that symmetric and transitive implies reflexive and the rest of the given proof is valid.)

9.11 Wlog we chose door 1. Now the prize has an equal chance of being behind each door, so there is a $\frac{1}{3}$ chance it is behind door 1, and a $\frac{2}{3}$ chance it is behind doors 2 or 3. So if we do not switch then we have a $\frac{1}{3}$ chance of success. However if the prize is behind doors 2 or 3 then the door it is not behind will be openned, leaving a $\frac{2}{3}$ chance it is behind the unopenned door, and this is our chance of success if we switch. So it is worth switching.

This answer may seem counter-intuitive because you might expect that the two remaining unopenned doors are equivalent and so must have an equal chance of containing the prize. This is in fact not the case; the distinguishing feature between the two is that the one you did not chose had the opportunity to be openned by the host and was not, which may have resulted from it containing the prize.

Alternatively we can use Bayes' theorem; wlog we chose door 1 and then the host opens door 2; let $P1$, $P2$, $P3$ be the events that the prize is behind doors 1, 2, 3 respectively and let $C1$, $C2$, $C3$ be the events that the host

opens doors 1, 2, 3 respectively,

$$\begin{aligned}
P(P1|C2) &= \frac{P(C2|P1)P(P1)}{P(C2|P1)P(P1) + P(C2|P2)P(P2) + P(C2|P3)P(P3)} \\
&= \frac{(1/2)(1/3)}{(1/2)(1/3) + 0(1/3) + 1(1/3)} \\
&= \frac{1/6}{1/2} \\
&= \frac{1}{3} \\
P(P2|C2) &= \frac{P(C2|P2)P(P2)}{P(C2|P1)P(P1) + P(C2|P2)P(P2) + P(C2|P3)P(P3)} \\
&= \frac{0(1/3)}{(1/2)(1/3) + 0(1/3) + 1(1/3)} \\
&= 0 \\
P(P3|C2) &= \frac{P(C2|P3)P(P3)}{P(C2|P1)P(P1) + P(C2|P2)P(P2) + P(C2|P3)P(P3)} \\
&= \frac{1(1/3)}{(1/2)(1/3) + 0(1/3) + 1(1/3)} \\
&= \frac{1/3}{1/2} \\
&= \frac{2}{3}
\end{aligned}$$

so we should switch to door 3.

9.22 There are $(n+2)!$ possible ways to order the people in a line. To enumerate the positions with k people between A and B first choose which of A and B comes leftmost (2 ways) then which place from the left A goes in $(n+1-k$ ways) which also determines which place B is in; finally have $n!$ ways to place the n other people in the remaining positions. So the

probability is $\frac{2(n+1-k)n!}{(n+2)!} = \frac{2(n+1-k)}{(n+1)(n+2)}$. Now check these sum to one,

$$\begin{aligned}\sum_{k=0}^{n} \frac{2(n+1-k)}{(n+1)(n+2)} &= \frac{2}{(n+1)(n+2)} \sum_{k=0}^{n} n+1-k \\ &= \frac{2}{(n+1)(n+2)} \left((n+1)(n+1) - \frac{1}{2} n(n+1) \right) \\ &= \frac{1}{n+2}[2(n+1)-n] \\ &= \frac{n+2}{n+2} \\ &= 1\end{aligned}$$

6.29 By the Fundemental Theorem of Arithmetic take prime factorisations $a = p_1^{a_1} ... p_n^{a_n}$ and $b = q_1^{b_1} ... q_n^{b_n}$ (if necessary some of the a_i and b_i may be zero. Then,

$$\begin{aligned}\text{lcm}(a,b)\text{gcd}(a,b) &= (p_1^{\max(a_1,b_1)} ... p_n^{\max(a_n,b_n)})(p_1^{\min(a_1,b_1)} ... p_n^{\min(a_n,b_n)}) \\ &= p_1^{\max(a_1,b_1)+\min(a_1,b_1)} ... p_n^{\max(a_n,b_n)+\min(a_n,b_n)} \\ &= p_1^{a_1+b_1} ... p_n^{a_n+b_n} \\ &= ab\end{aligned}$$

6.45 We want to express $7x + 13y = 500$ for $-500 \leq x, y \leq 500$ (we can simulate x and y negative by placing weights on the same side of the scale as the gold). Note that $2.7 - 13 = 1$ (by observation or Euclid's algorithm) so $1000.7 - 500.13 = 500$. However this uses too many weights. Note that $13.7 = 7.13$ so $650.7 = 350.13$ and removing these weights gives a solution $350.7 - 150.13 = 500$.

To solve the second part we would need integers x and y such that $6x + 9y = 500$. However note that $\text{GCD}(6, 9) = 3$ and 3 does not divide 500 so as we saw in classs this is impossible. Alternatively observe directly that the left hand side of the equation must be divisible by 3 and the right hand side is not.

6.53 First note that if the game is played through to the end, then after Bs last move the total value of played cards is $1 + ... + 2n = 2n(2n + 1)$ which is divisible by $2n + 1$. So B just has to make sure after each of his turn that A cannot win immediately and B is guaranteed to win eventually. Note also that B knows which cards A has in hand; they consist of everything that

has not been played and that B does not have in hand. Note further that A cannot win on his first turn as none of the cards by themselves is divisible by $2n+1$.

On each of B's turns, for each card k remaining in A's hand he must avoid making a total of the form $-k(\text{mod } 2n+1)$. So he has to avoid one congruence class for each card A has left. But B has one more card left than A does, and each will give a total in a different congruence class, so he is guaranteed a card that yields a congruence class from which A cannot win.

Extra 1 $1001!+2, 1001!+3, ..., 1001!+1001$ are all composite.

Extra 2 Suppose there are only finitely many primes of the form $4n-1$, enumerate them as $p_1, ..., p_k$ and consider $4p_1...p_k - 1$. It has a prime factorisation, and this does not include any of the p_i and does not include 2, leaving us only with primes of the form $4n+1$. However note that if we multiply together two numbers $4n+1$ and $4m+1$ of this form we get $(4n+1)(4m+1) = 4(4nm+m+n)+1$ which is another number of the same form. So there is no way to build $4p_1...p_k - 1$ from primes of this form alone.

This reasoning does not work to prove there are infinitely many primes of the form $4n+1$ because $(4n-1)(4m-1) = 4(4mn+m+n)+1$ so we can build either type of odd number by multiplying together primes of the form $4n-1$ and we needn't care that we have run out of those of the form $4n+1$.