Discrete Structures — *Final exam sample questions— **Solutions***
CS2800 — *Questions selected for fall 2017*

1. *Determine the prime factorizations, greatest common divisor, and least common multiple of the following pairs of numbers (m, n). In each case, give Bézout coefficients s and t such that $sm + tn = gcd(m, n)$.*

   (a) $(6, 8)$ *prime factorizations* $= \boxed{2 \cdot 3}\ \boxed{2^3}$

   $gcd = \boxed{2}$ $lcm = \boxed{24}$ $s = \boxed{-1}$ $t = \boxed{1}$

   (b) $(5, 7)$ *prime factorizations* $= \boxed{5}\ \boxed{7}$

   $gcd = \boxed{1}$ $lcm = \boxed{35}$ $s = \boxed{3}$ $t = \boxed{-2}$

   (c) $(21, 12)$ *prime factorizations* $= \boxed{3 \cdot 7}\ \boxed{2^2 \cdot 3}$

   $gcd = \boxed{3}$ $lcm = \boxed{84}$ $s = \boxed{-1}$ $t = \boxed{2}$

2. *Prove that $7^m - 1$ is divisible by 6 for all positive integers m.*

   Solution There are two ways to do this. One way: notice that $7 \equiv 1 \mod 6$, thus $7^m \equiv 1 \mod 6$ for any m (applying the known result that "if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$" $m - 1$ times), and thus $7^m - 1 \equiv 0 \mod 6$. This implies $7^m - 1$ is divisible by 6.

   Alternatively you can do a direct proof by induction:

   Base case: $m = 1$, $7^1 - 1 = 6$ which is obviously divisible by 6.

   Inductive step: Assume $7^m - 1$ is divisible by 6 for some $m \geq 1$ (inductive hypothesis). Then $7^{m+1} - 1 = 7^{m+1} - 7 + 6 = 7(7^m - 1) + 6$. But $7^m - 1$ is divisible by 6 (by the inductive hypothesis) and so is 6, so $7^{m+1} - 1$ is also divisible by 6. Hence proved by induction.

3. *Suppose that Alice sends the message a to Bob, encrypted using RSA. Suppose that Bob's implementation of RSA is buggy, and computes $k^{-1} \mod 4\phi(m)$ instead of $k^{-1} \mod \phi(m)$. What decrypted message does Bob see? Justify your answer.*

   Solution Alice transmits $a^k \mod m$ to Bob, who then computes $(a^k)^{k^{-1}} \mod m$. Because Bob miscomputed k^{-1}, we know that $kk^{-1} \equiv 1 \mod 4\phi(m)$. In other words, $kk^{-1} = 1 + t \cdot 4\phi(m)$ for some t. Therefore Bob receives

$$\begin{aligned}(a^k)^{k^{-1}} &\equiv a^{1+4t\phi(m)} \\ &\equiv a \cdot a^{4t\phi(m)} \\ &\equiv a \cdot (a^{\phi(m)})^{4t} \\ &\equiv a \cdot 1^{4t} \\ &\equiv a \mod m\end{aligned}$$

4. *(a) What are the units of $\mathbb{Z}$ mod 12?*

Solution A unit in a set of numbers is a number that has an inverse. In the set $\mathbb{Z}_{12} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8]$ the units are [1], [5], [7], and [11]. In general, $[n]$ is a unit mod m if n and m are relatively prime.

(b) What are their inverses?

Solution $[1]^{-1} = [1]$, $[5]^{-1} = [5]$, $[7]^{-1} = [7]$, and $[11]^{-1} = [11]$. This is because $[1] \cdot [1] = [1]$, $[5] \cdot [5] = [25] = [1]$, $[7] \cdot [7] = [49] = [1]$ and $[11] \cdot [11] = [121] = 1$.

(c) What is $\phi(12)$?

Solution By definition of ϕ, $\phi(12)$ is the number of units mod 12. Since there are 4 units, $\phi(12) = 4$.

5. *Use Euler's theorem and repeated squaring to efficiently compute* $8^n \mod 15$ *for* $n = 5$, $n = 81$ *and* $n = 16023$. *Hint: you can solve this problem with 4 multiplications of single digit numbers. Please fully evaluate all expressions for this question (e.g. write 15 instead of* $3 \cdot 5$*).*

Solution We use the fact that $8^{\phi(15)} = 1 \mod 15$. $\phi(15) = (3-1)(5-1) = 8$ [multiplication #1], so we can reduce all of the exponents mod 8. We then use repeated squaring to compute 8^{2^k}:

$$\begin{aligned} &[8]^1 = [8] \\ &[8]^2 = [64] = [4] && \text{[multiplication \#2]} \\ &[8]^4 = [4]^2 = [16] = [1] && \text{[multiplication \#3]} \end{aligned}$$

We can then use these to compute the powers of [8]:

$$\begin{aligned} [8]^5 &= [8]^4[8] = [1][8] = [8] \\ [8]^{81} &= [8]^1 = [8] \\ [8]^{16023} &= [8]^7 = [8]^4[8]^2[8] = [1][4][8] = [32] = [2] && \text{[multiplication \#4]} \end{aligned}$$

6. *Compute* $10101b + 101b$ *(recall that* b *indicates the strings of digits should be interpreted as integers using the binary representation). Express your answer in both binary and decimal.*

Solution There are two approaches:

Adding in binary, we have

$$\begin{array}{rcccccc} & & 1 & & 1 & & \\ & 1 & 0 & 1 & 0 & 1 & \text{b} \\ + & & & 1 & 0 & 1 & \text{b} \\ \hline & 1 & 1 & 0 & 1 & 0 & \text{b} \end{array}$$

Converting this to decimal gives $0 + 2 + 0 + 8 + 16 = 26$.

Alternatively, we could convert to decimal, then add, then convert back: $10101b = 1 + 4 + 16 = 21$ and $101 = 1 + 4 = 5$. Adding these gives $26 = 16 + 8 + 2 = 11010b$.

7. *In this problem, we are working mod 7, i.e.* $\equiv$ *denotes congruence mod 7 and* $[a]$ *is the equivalence of* a *mod 7.*

(a) What are the units of $\mathbb{Z}_7$*? What are their inverses?*

Solution

- $[1]$'s inverse is $[1]$
- $[2]$'s inverse is $[4]$
- $[3]$'s inverse is $[5]$
- $[4]$'s inverse is $[2]$
- $[5]$'s inverse is $[3]$
- $[6]$'s inverse is $[6]$

(b) *Compute* $[2]^{393}$.

Solution $[2]^{393} = ([2]^3)^{131} = [1]^{131} = [1]$

8. *Suppose you are given a function* $f : \mathbb{N} \to \mathbb{N}$, *and are told that* $f(1) = 1$ *and for all* n, $f(n) \leq 2f(\lfloor n/2 \rfloor) + 1$.

Use strong induction on n *to prove that for all* $n \geq 2$, $f(n) \leq 2n \log_2 n$.

You may write $\log$ *to indicate* $\log_2$. *Here is a reminder of some facts about* $\lfloor x \rfloor$ *and* $\log x$*:*

- $\lfloor x \rfloor \leq x$
- $\log 1 = 0$, $\log 2 = 1$
- $\log(x/2) = \log x - 1$
- $\log(2^x) = x$
- $\log(x^2) = 2 \log x$
- *if* $x \leq y$ *then* $\log x \leq \log y$

Solution In the base case, we need to show $f(2) \leq 4 \log 2 = 2$. But we are given that $f(2) \leq 2f(1) + 1 = 3 \leq 4$, as required.

For the inductive step, choose $n > 2$, and assume that for all $k < n$, $f(k) \leq 2k \log k$. We must show that $f(n) \leq 2n \log n$.

We compute:

$$\begin{aligned}
f(n) &\leq 2f(\lfloor n/2 \rfloor) + 1 && \text{given} \\
&\leq 4\lfloor n/2 \rfloor \log \lfloor n/2 \rfloor + 1 && \text{by inductive hypothesis} \\
&\leq 4(n/2) \log \lfloor (\rfloor n/2) + 1 && \text{by facts stated in question} \\
&\leq 2n \log n - 2n + 1 \leq 2n \log n + (1 - 2n) && \text{arithmetic} \\
&\leq 2n \log n + 0 && \text{since } n > 2 \text{ so } 1 - 2n < 0 \\
&= 2n \log n && \text{as required.}
\end{aligned}$$

9. (a) *Recall Bézout's identity from the homework: for any integers* n *and* m, *there exist integers* s *and* t *such that* $gcd(n, m) = sn + tm$. *Use this to show that if* $gcd(k, m) = 1$ *then* $[k]$ *is a unit of* $\mathbb{Z}_m$.

Solution If $gcd(k, m) = 1$ then $1 = sk + tm$. Reducing this equation mod m gives $[1] = [s][k] + [t][0] = [s][k]$. Therefore, $[k]$ has an inverse (namely $[s]$); and is thus a unit.

(b) *Use part (a) to show that if* p *is prime, then* $\phi(p) = p - 1$.

Solution Since p is prime, everything less than p is relatively prime to p, except for 0. There are $p - 1$ such numbers, and thus $p - 1$ units.

(c) *Use Euler's theorem to compute* $3^{38} \mod 37$ *(note: 37 is prime).*

Solution $\phi(37) = 36$, so $[3]^{38} = [3]^2 = [9] \bmod 37$.

10. *Bob the Bomber wishes to receive encrypted messages from Alice the Accomplice. He generates a public key pair $m = 21$ and $k = 5$. Luckily, you have access to an NSA supercomputer that was able to factor* 21 *into* $7 \cdot 3$.

    (a) *Use this information to find the decryption key k^{-1}.*

    Solution We must find the inverse of 5 mod $\phi(m) = \phi(7 \cdot 4) = (7-1)(4-1) = 12$. Experimentally, $[5 \cdot 5] = [25] = [1]$. Alternatively, you can use the pulverizer. This results in $1 = -2 \cdot 12 + 5 \cdot 5$, giving an inverse of 5.

    (b) *Without changing m, what other possible keys k could Bob have chosen? Find the decryption keys for those keys as well.*

    Solution By inspection, the units of $\mathbb{Z}_{12}$ are [1], [5], [7], and [11] (all other numbers share a factor with 12). Experimentally, they are all their own inverses. Note that [1] is not a smart key choice, but we accepted it.

    (c) *Alice encrypts a secret message msg using Bob's public key ($k = 5$), and sends the ciphertext $c = 4$. What was the original message?*

    Solution We must compute $[4]^{[5]} = [4^5]$. We see $[4^2] = [16]$; squaring this gives $[4^4] = [(4^2)^2] = [256] = [4]_{21}$. Thus $[4^5] = [4 \cdot 4^4] = [16]$.

11. *(a) Explain carefully what the flaw is with the following "proof" that every postage of three cents or more can be formed using just three-cent and four-cent stamps.*

    We use regular induction to prove that $P(n)$ holds for all $n \geq 3$, where $P(n)$ says that postage of n cents cents can be formed using just three-cent and four-cent stamps.

    Base Case: *We can form postage of three cents with a single three-cent stamp and we can form postage of four cents using a single four-cent stamp.*

    Inductive Step: *Assume that we can form postage of j cents for all nonnegative integers j with $j \leq k$ using just three-cent and four-cent stamps. We can then form postage of $k + 1$ cents by replacing one three-cent stamp with a four-cent stamp or by replacing two four- cent stamps by three three-cent stamps.*

    (b) Show that every postage of six cents or more can be formed using just three-cent and four-cent stamps.

    Solution (a) In doing the inductive step, you don't know that a three-cent stamp or two four-cent stamps were used in paying for k cents. In particular, if $k = 4$, only one four-cent stamp is used. So the argument going from 4 to 5 fails. (We also reluctantly accepted as an error in the proof that the inductive step should have said "Assume that we can form postage of j cents for all nonnegative integers j with $3 \leq j \leq k$"; that is, we mut start at 3 (because that's the base case), not 0 (which is what we're doing if we just say "for all nonnegative integers j with $j \leq k$".)

    (b) Use strong induction to prove $P(n)$ (where $P(n)$ is as above) for $n \geq 6$.

    Base Case: We can form postage of six cents using two three-cent stamps.

    Inductive Step: Suppose that $P(j)$ holds for all $j \leq n$. We want to prove $P(n + 1)$.

    If $n + 1 = 7$, we can use a three- and a four-cent stamp; if $n + 1 = 8$, we can use two four-cent stamps. (It's OK to make 7 and 8 part of the base case.) If $n + 1 \geq 9$, then $n \geq 8$, so $n + 1 - 3 = n - 2 \geq 6$. That means that, using the induction hypothesis, we can pay for $n - 2$ cents of postage using three- and four-cent stamps. Add one more three-cent stamp. That will pay for $n + 1$ cents of postage.

As in question 3, we deducted points for including "for all n" in the statement $P(n)$ or somehow treating $P(n)$ as a number.

12. *Complete the following proof.*

    Claim: *For all $k > 0$ and all $a, b \geq 0$, $gcd(ka, kb) = k \cdot gcd(a, b)$.*

    Proof: *By (strong) induction on b. Let $P(b)$ be the statement "for all $k > 0$ and all a, $gcd(ka, kb) = k \cdot gcd(a, b)$."*

    $P(0)$ is clearly true: $gcd(ka, kb) = gcd(ka, 0) = ka = k \cdot gcd(a, 0)$.

    *For the inductive step, assume $P(0)$, $P(1)$, $\ldots P(b-1)$. We wish to show $P(b)$. Use Euclidean division to write $a = qb + r$ with $0 \leq r < b$. By Euclid's algorithm, we know $g(a, b) =$ **[FILL IN]**. Similarly $g(ka, kb) =$**[FILL IN]** where **[FILL IN]**.*

    [FILL IN]

    Therefore $gcd(ka, kb) = k \cdot gcd(a, b)$.

Solution **Proof:** By (strong) induction on b. Let $P(b)$ be the statement "for all $k > 0$ and all a, $gcd(ka, kb) = k \cdot gcd(a, b)$."

$P(0)$ is clearly true: $gcd(ka, kb) = gcd(ka, 0) = ka = k \cdot gcd(a, 0)$.

For the inductive step, assume $P(0)$, $P(1)$, $\ldots P(b-1)$. We wish to show $P(b)$. Use Euclidean division to write $a = qb + r$ with $0 \leq r < b$. By Euclid's algorithm, we know $g(a, b) = g(b, r)$. Similarly $g(ka, kb) = g(kb, r')$ where $ka = kbq' + r'$.

We want to show that $g(ka, kb) = kg(a, b)$. By the inductive hypothesis, since $r < b$, we know that $g(kb, kr) = kg(b, r) = kg(a, b)$. We would therefore be done if we could show that $r' = kr$.

However, we know that $ka = kbq' + r'$ (where $0 \leq r' < kb$) and also that $ka = kbq + kr$ (where $0 \leq kr < kb$). By the uniqueness of the quotient and remainder of ka by kb, we see that $r' = kr$.

Therefore, $gcd(ka, kb) = gcd(kb, r') = gcd(kb, kr) = k \cdot gcd(b, r) = k \cdot gcd(a, b)$.

13. *Prove by induction that $3^{2n-1} + 1 \equiv 0$ (mod 4) for all $n \geq 1$.*

Solution Let $P(n)$ be the statement $3^{2n-1} + 1 \equiv 0$ (mod 4). $P(1)$ says that $3 + 1 \equiv 0$ (mod 4), which is clearly true. Suppose that $P(n)$ holds; that is $3^{2n-1} + 1 \equiv 0$ (mod 4), or equivalently, $3^{2n-1} \equiv -1$ (mod 4). We want to show that $P(n+1)$ holds. $P(n+1)$ says that $3^{2n+1} + 1 \equiv 0$ (mod 4). Now $3^{2n+1} = 93^{2n-1}$. By the induction hypothesis, $3^{2n-1} \equiv -1$ (mod 4). Note that $9 \equiv 1$ (mod 4). It follows that $3^{2+1} = 9 \times 3^{2n-1} \equiv 1 \times -1 \equiv -1$ (mod 4). Thus, $3^{2n+1} + 1 \equiv 0$ (mod 4).

14. (a) *Build a proof tree showing that $\vdash \neg(P \lor Q) \to \neg P$. You may refer to the list of rules given at the end of the exam.*

Solution

$$\dfrac{\dfrac{\dfrac{}{\cdots \vdash P \lor \neg P}\;excl\ mid \qquad \dfrac{\dfrac{\dfrac{}{\cdots \vdash P}\;assum}{\cdots \vdash (P \lor Q)}\;\lor intro \qquad \dfrac{}{\cdots \vdash \neg(P \lor Q)}\;assum}{\ldots, P \vdash \neg P}\;absurd \qquad \dfrac{}{\ldots, \neg P \vdash \neg P}\;assum}{\neg(P \lor Q) \vdash \neg P}\;\lor elim}{\vdash \neg(P \lor Q) \to \neg P}\;\to intro$$

(b) *Show, using truth tables, that $\models \neg(P \lor Q) \to \neg P$.*

Solution Here is the truth table for $\neg(P \vee Q) \to \neg P$:

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P$	$\neg(P \vee Q) \to \neg P$
T	T	T	F	F	T
T	F	T	F	F	T
F	T	T	F	T	T
F	F	F	T	T	T

As you can see, every row of the truth table is true.

15. *Because we reordered the topics this semester, past semesters have not had many questions on logic. A good exercises is to use truth tables to find valid statements and then build proof trees for them. For example, you might prove* $P \to (Q \to R) \vdash P \wedge Q \to R$*, or* $P \to Q \vdash Q \vee \neg P$ *or* $\vdash \neg(P \wedge Q) \to (\neg P \vee \neg Q)$.

Solution

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\cdots \vdash P \to (Q \to R)}\,\text{assum} \qquad \dfrac{\dfrac{}{\cdots \vdash P \wedge Q}\,\text{assum}}{\cdots \vdash P}\,\wedge\text{ elim}}{\cdots \vdash (Q \to R)}\,\to\text{ elim} \qquad \dfrac{\dfrac{}{\cdots \vdash P \wedge Q}\,\text{assum}}{\cdots \vdash Q}\,\wedge\text{ elim}}{\cdots, P \wedge Q \vdash R}\,\to\text{ elim}}{P \to (Q \to R) \vdash P \wedge Q \to R}\,\to\text{ intro}$$

$$\dfrac{\dfrac{}{\cdots \vdash P \vee \neg P}\,\text{ex. mid.} \qquad \dfrac{\dfrac{\dfrac{}{\cdots \vdash P \to Q}\,\text{assum} \qquad \dfrac{}{\cdots \vdash P}\,\text{assum}}{\cdots \vdash Q}\,\to\text{ elim}}{\cdots, P \vdash Q \vee \neg P}\,\vee\text{ intro} \qquad \dfrac{\dfrac{}{\cdots \vdash \neg P}\,\text{assum}}{\cdots, \neg P \vdash Q \vee \neg P}\,\vee\text{ elim}}{P \to Q \vdash Q \vee \neg P}\,\vee\text{ elim}$$

$$\dfrac{\dfrac{\dfrac{}{\cdots \vdash P \vee Q}\,\text{ex. mid.} \qquad \dfrac{\dfrac{\dfrac{}{\cdots \vdash Q \vee \neg Q}\,\text{ex. mid.} \qquad \dfrac{\textit{below}}{\cdots, Q \vdash \neg Q} \qquad \dfrac{}{\cdots, \neg Q \vdash \neg Q}\,\text{assum}}{\cdots \vdash \neg Q}\,\vee\text{ elim}}{\cdots, P \vdash \neg P \vee \neg Q}\,\vee\text{ intro} \qquad \dfrac{\dfrac{}{\cdots \vdash \neg P}\,\text{assum}}{\cdots, \neg P \vdash \neg P \vee \neg Q}\,\vee\text{ intro}}{\neg(P \wedge Q) \vdash \neg P \vee \neg Q}}{\vdash \neg(P \wedge Q) \to (\neg P \vee \neg Q)}\,\to\text{ intro}$$

$$\dfrac{\dfrac{\dfrac{}{\cdots \vdash P}\,\text{assum} \qquad \dfrac{}{\cdots \vdash Q}\,\text{assum}}{\cdots \vdash P \wedge Q}\,\wedge\text{ intro} \qquad \dfrac{}{\cdots \vdash \neg(P \wedge Q)}\,\text{assum}}{\neg(P \wedge Q), P, Q \vdash \neg Q}\,\text{absurd}$$

16. *Explain carefully what the bug is in the following argument:*

> *We prove by strong induction that all orders of fish for at least 6 pounds of fish can be filled using only 3-pound fish. Let* $P(n)$ *be the statement that an order of fish for* n *pounds of fish can be filled using only 3-pound fish. We prove* $P(n)$ *for* $n \geq 6$*. Clearly* $P(6)$ *is true: an order for 6 pounds of fish can be filled using two 3-pound fish. Suppose that* $P(6), \ldots, P(n)$ *are all true. We prove* $P(n+1)$*. We want to show that we can fill an order for* $n+1$ *pounds of fish using 3-pound fish, if* $n \geq 6$*. By the induction hypothesis, we can fill an order for* $n-2$ *pounds of fish using 3-pound fish. Add one more 3-pound fish, and we've filled the order for* $n+1$ *pounds. This completes the induction argument.*

Solution The problem comes when $n = 6$ and we're trying to prove $P(n + 1)$, that is, $P(7)$. At this point we get to assume only that $P(6)$ is true. But the proof assumes that $P(n - 2)$, which is $P(4)$ if $n = 6$, is true. We don't get to assume this (and, indeed, $P(4)$ is false).

[Although you didn't have to say this, note that we could have tried to fix the problem by taking $P(6)$, $P(7)$, and $P(8)$ as base cases. In that case, the inductive step would work, but the base case would fail (since $P(7)$ and $P(8)$ are false).]

17. *[4 points] Which of the following does RSA depend on? Explain your answer briefly.*

    (a) Factoring is easy and testing primality is hard.

    (b) Factoring is hard and testing primality is easy.

    (c) Both factoring and testing primality are hard.

    (d) Both factoring and testing primality are easy.

Solution RSA depends on (b), that factoring is hard and testing primality is easy. The public key in RSA is the product of two large primes. We couldn't generate public keys if testing primality wasn't easy. On the other hand, we could easily decrypt encrypted messages if factoring was easy (because in that case, given a public key, which is the product of two large primes could easily compute the secret – the two factors, and that's what we need to know to decrypt.

18. *(a) Let m and n be integers greater than 1. Show that the function $f : \mathbb{Z}_m \times \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ given by $f : ([a]_m, [b]_n) \rightarrow [a + b]_m$ is not necessarily well defined. [Hint: you just need an example here.]*

    Solution Consider $m = 2$, $n = 3$. Then $[1]_m = [3]_m$ and $[1]_n = [4]_n$, but $[1 + 3]_m = [0]_m$ while $[3 + 4]_m = [1]_m$.

    (b) Show that f is well defined if $m|n$.

    Solution Suppose $m|n$. Then $n = mc$ for some c. Suppose also that $[a]_m = [a']_m$ (so that $a = a' + md$ for some d) and $[b]_n = [b']_n$ (so that $b = b' + ne$).

    Then
    $$a + b = (a' + md) + (b' + ne) = a' + b' + md + mce = a' + b' + m(d + ce)$$

    Thus $[a + b]_m = [a' + b']_m$.

19. *For $n \geq 0$, let $F_n = 2^{2^n} + 1$. (Those numbers F_n which are prime are called* Fermat primes.*)*

    (a) [5 points] Prove by induction that $\prod_{r=0}^{n-1} F_r = F_n - 2$.

    Solution (a) Let $P(n)$ be the statement $\prod_{r=0}^{n-1} F_r = F_n - 2$. We prove $P(n)$ for all $n \geq 1$ by induction.

    Base case: $P(1)$ says that $\prod_{r=0}^{0} F_r = F_1 - 2$. Since $F_0 = 2^{2^0} + 1 = 3$ and $F_1 = 2^{2^1} + 1 = 5$, we have $F_0 = F_1 - 2$, so the base case holds.

    Inductive step. Assume $P(n)$. We must prove $P(n + 1)$, which says that $\prod_{r=0}^{n} F_r = F_{n+1} - 2$.

$$\begin{array}{rcll}
\prod_{r=0}^{n} F_r & = & (\prod_{r=0}^{n-1} F_r)F_n & \\
 & = & (F_n - 2)F_n & \text{[induction hypothesis]} \\
 & = & (2^{2^n} + 1 - 2)(2^{2^n} + 1) & \\
 & = & (2^{2^n} - 1)(2^{2^n} + 1) & \\
 & = & (2^{2^n})^2 - 1 & \\
 & = & 2^{2 \cdot 2^n} - 1 & \\
 & = & 2^{2^{n+1}} - 1 & \\
 & = & (2^{2^{n+1}} + 1) - 2 & \\
 & = & F_{n+1} - 2 &
\end{array}$$

This completes the proof by induction.

(b) [5 points] Prove that $\gcd(F_m, F_n) = 1$ *for all* m, n *with* $m < n$. *(Hint: use part (a)—which you can use even if you haven't proved it—and some standard facts about divisibility.)*

Solution Suppose that $m < n$. By part (a), $F_n = \prod_{r=0}^{n-1} F_r + 2$. Thus, $\gcd(F_m, F_n) = \gcd(F_m, \prod_{r=0}^{n-1} F_r + 2)$. Thus, the remainder when we divide F_n by F_m is 2 (since F_m is a factor of $\prod_{r=0}^{n-1} F_r 2$). By Euclid's algorithm,

$$\gcd(F_m, \prod_{r=0}^{n-1} F_r + 2) = \gcd(2, F_m) = \gcd(2, 2^{2^m} + 1) = \gcd(1, 2) = 1.$$