Math 567, Assignment #1: Solutions

1. The proof is by induction on n. $\frac{1}{1^2} \le 2 - \frac{1}{1}$, so the claim holds for $n = 1$. Now suppose the claim holds for some particular n, so that $\frac{1}{1^2} + \ldots + \frac{1}{n^2} \le 2 - \frac{1}{n}$. Then $\frac{1}{1^2} + \ldots + \frac{1}{n^2} + \frac{1}{(n+1)^2} \le 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \le 2 - \frac{1}{n+1}$ (where the last inequality follows from the easy inequality $(n+1)^2 - n \ge n(n+1)$ by dividing both sides by $n(n+1)^2$ and subtracting the resulting expressions from 2). Hence the claim holds for $n+1$ as well. The inequality therefore is true for all n, by induction.

2. The following explanations are wordier than yours need to be, but I want to be a bit verbose to illustrate the variety of approaches that can be used for problems like this.

(a) First find the gcd: $(18,5) \to (5, 18 - 3 \cdot 5) = (5,3) \to (3, 5-3) = (3,2) \to (2, 3-2) = (2,1) = (1, 2 - 2 \cdot 1) = (1,0)$. Then retrace to express the gcd as a difference of multiples of 18 and 5: $3 = 18 - 3 \cdot 5$, $2 = 5 - 3 = 5 - (18 - 3 \cdot 5) = 4 \cdot 5 - 18$, $1 = 3 - 2 = (18 - 3 \cdot 5) - (4 \cdot 5 - 18) = 2 \cdot 18 - 7 \cdot 5$. Then scale up to get $48 = 18(2 \cdot 48) - 5(7 \cdot 48)$. So one solution to $18x + 5y = 48$ is $x_0 = 96$, $y_0 = -336$. The general solution in integers is thus $x = 96 - 5t$, $y = -336 + 18t$, with t an integer. To make x, y positive, we need $5t \le 96$ (i.e., $t \le 19$) and $18t \ge 336$ (i.e., $t \ge 19$). So a simpler integer solution is the unique solution in non-negative integers, namely $x_1 = 96 - 95 = 1$, $y_1 = -336 + 342 = 6$. We may write the general solution in terms of this particular solution, rather than the one we originally found: $x = 1 + 5t$, $y = 6 - 18t$ (a different t from before). Note, by the way, that it is perfectly legitimate to obtain the solution $x = 1, y = 6$ by systematic or intuitive guess-work. Indeed, if one knows or suspects ahead of time that a simple solution exists, trial and error may be the fastest way of finding a particular solution.

(b) Divide the equation by gcd(54,21,906), or 3, to obtain $18x + 7y = 302$. To find (x_0, y_0), we can repeatedly reduce 302 by 18's until we obtain a multiple of 7:

302 leaves a remainder of 1 (when divided by 7);
284 leaves a remainder of 4; and
266 leaves a remainder of 0.

$302 - 2 \cdot 18 = 266 = 38 \cdot 7$, so $x_0 = 2$, $y_0 = 38$ is one solution, and the general solution is of the form $x = 2 + 7t$, $y = 38 - 18$. To get a positive integer solution, we need $t \geq 0$ and $t \leq 2$, so (2,38), (9,20), and (16,2) are the only solutions in positive integers.

(c) We can "over-subtract" when that helps us, as it does here. $\gcd(360, 123) = \gcd(123, 360 - 3 \cdot 123) = \gcd(123, -9) = gcd(123, 9)$. But wait: 9 divides 99, which is the number we're trying to express in terms of 360s and 123s. We have $9 = 3{\cdot}123 - 360$, so, multiplying by 11, we get $99 = 33{\cdot}123 - 11{\cdot}360$. Since $\gcd(123, 360) = 3$ (check!), the general solution is $x = 33 - \frac{360}{3}t = 33 - 120t$, $y = -11 + \frac{123}{3}t = -11 + 41t$. To get a solution in positive integer, we need $t < 33/120$ and $t > 11/41$. No such whole number t exists, so there are no solutions in positive integers.

(d) Here's a different approach for part (d): For some small value of m (might as well take $m = 1$), we write $158m$ as some multiple of 57, plus or minus a small amount:

$$1 \cdot 158 - 3 \cdot 57 = -13.$$

Scale this up by a factor close to $57/13 \approx 4$:

$$4 \cdot 158 - 12 \cdot 57 = -52.$$

Then adding 57 gives

$$4 \cdot 158 - 11 \cdot 57 = 5.$$

Now we want to combine some multiple of the ... $= -13$ equation with some multiple of the ... $= 5$ equation so that the RHS becomes 7. That is, we need to find a multiple of 13 and a multiple of 5 whose difference is 7. 52 and 45 will do, so our multipliers are 4 and 9, respectively.

$$4 \cdot 158 - 12 \cdot 57 = -52$$

$$36 \cdot 158 - 99 \cdot 57 = 45$$

Adding, we get

$$40 \cdot 158 - 111 \cdot 57 = -7$$

so

$$-40 \cdot 158 + 111 \cdot 57 = 7.$$

Thus we can take $x_0 = -40$, $y_0 = -111$ as our basic solution. Since $\gcd(158, 57) = 1$ (check!), the general solution is $x_0 = -40 + 57t$, $y_0 =$

$-111 + 158t$. The smallest positive solution is $x = -40 + 57 = 17$, $y = -111 + 158 = 47$, and the general solution in positive integers can be written as $x = 17 + 57t$, $y = 47 + 158t$ with $t \geq 0$.

3. We use the division algorithm.

(a) $\gcd(2a+1, 9a+4) = \gcd(2a+1, (9a+4) - 4 \cdot (2a+1)) = \gcd(2a+1, a) = \gcd(a, (2a+1) - 2 \cdot a) = \gcd(a, 1) = 1$.

(b) $\gcd(5a+2, 7a+3) = \gcd(5a+2, (7a+3) - (5a+2)) = \gcd(5a+2, 2a+1) = \gcd(2a+1, 5a+2-2 \cdot (2a+1)) = \gcd(2a+1, a) = 1$ as above.

(c) $\gcd(3a, 3a+2) = \gcd(3a, (3a+2) - 3a) = \gcd(3a, 2)$. The only (positive) divisors of 2 are 1 and 2. If a is odd, then since the prime 2 does not divide a or 3, 2 does not divide $3a$, when $\gcd(3a, 2) = 1$.

4. Let d be the gcd of n^2+1 and $n+2$. If $\frac{n^2+1}{n+2}$ is an integer, then $d = n+2$. On the other hand, $\gcd(n^2+1, n+2) = \gcd(n+2, (n^2+1) - n \cdot (n+2)) = \gcd(n+2, 1-2n)$, so d must divide $n+2$ and $1-2n$. It follows that d divides $2(n+2) + (1-2n) = 5$, so $n+2$ (which equals d) must be one of the four numbers $+1, -1, +5, -5$ (which are the four divisors of 5). This gives the solutions $n = -7, -3, -1, 3$.

5. (a) If n is not a power of 2, it must have an odd prime factor p. Then, writing $n = mp$ and $2^n = (2^m)^p$, we have $2^n + 1 = (2^m)^p + 1$; putting $M = 2^m$, this expression is $M^p + 1$, which factors as $(M+1)(M^{p-1} - M^{p-2} + \cdots - M + 1)$. The factor $M+1$ is bigger than 1 but less than $M^p + 1$, so $M^p + 1$ cannot be prime.

(b) Suppose $j < k$. If we multiply $2^{(2^j)} + 1$ by $2^{(2^j)} - 1$ we get $2^{(2^{j+1})} - 1$. If we multiply this by $2^{(2^{j+1})} + 1$, we get $2^{(2^{j+2})} - 1$. If we multiply this by $2^{(2^{j+2})} + 1$, we get $2^{(2^{j+3})} - 1$. Et cetera. In this fashion, we eventually arrive at the fact that $2^{(2^k)} - 1$ is a multiple of $2^{(2^j)} + 1$. Hence, if we divide $2^{(2^k)} + 1$ by $2^{(2^j)} + 1$, we get remainder 2. Therefore the gcd of $2^{(2^j)} + 1$ and $2^{(2^k)} + 1$ must a divisor of 2. But the two numbers in question are both odd. Hence the gcd must be 1.

6. Suppose n is not prime, so that it can be written as $n = km$ with k, m both bigger than 1. Write $M = 2^m$. Then $2^n - 1 = 2^{km} - 1 = M^k - 1 = (M-1)(M^{k-1} + M^{k-2} + \ldots + M + 1)$. The factor $M - 1$ is bigger than 1 (because $m > 1$ implies $2^m > 2$) and less than $M^k - 1$ (because $k > 1$), so $N^k - 1$ is not prime.

7. Lemma: The product of two or more integers of the form $3k+1$ is of the

same form. Proof: It is enough to prove the case of just two integers (since the general claim follows by induction). Simplfy check that the product of $3j + 1$ and $3k + 1$ is $9jk + 3j + 3k + 1$, which equals $3(3jk + j + k) + 1$.

Now, to prove that infinitely many primes are of the form $3k+2$, suppose that there were only finitely many such primes, say $p_1, p_2, \ldots, p_r$. Call their product N. $3N - 1$ cannot be divisible by any of the p_i's, nor can it be divisible by 3. Hence it must be a product of primes of the form $3k+1$. But any product of such primes must also be of that form, and $3N - 1$ is not. This contradiction establishes the claim.