Solutions to Assignment #3

p. 49, E2: Notice that this is a generalization of Lemma 2, which says that if a prime p divides a product of *two* factors then it must divide at least one of them.

Let P(n) be the assertion that if a prime p divides a product of n factors, i.e., $p|a_1a_2\ldots a_n$, then p divides (at least) one of the factors a_i. (Thus Lemma 2 is the case P(2).)

The problem doesn't say what starting n to use, but since P(1) is true, let's start there[1].

Proof by induction on n: P(1) says that if $p|a_1$ then $p|a_1$, which is trivially true.

Now assume that P(k) is true (the "inductive hypothesis") and consider P($k+1$). If $p|a_1\ldots a_ka_{k+1}$, we can view this as as $p|(a_1\ldots a_k)a_{k+1}$. By Lemma 2, p divides at least one of $(a_1\ldots a_k)$ and a_{k+1}. If $p|a_{k+1}$, we are done. If not, then $p|a_1\ldots a_k$, and by the inductive hypothesis p divides at least one of $a_1,\ldots,a_k$, so again we are done and P($k+1$) has been verified.

Therefore $P(n)$ is true for all $n \geq 1$ by mathematical induction. □

(A box like this is often used to mark the end of a proof.)

Notice that this kind of induction, where the case $n = 2$ is used to prove an assertion for general n, is very easy, even though it took a bit of writing to say it. So in this course and in more advanced mathematics courses, we'll often just say, "By Lemma 2 and induction, $p|a_1\ldots a_n$ implies $p|a_i$ for some i" and not give details. You may do the same, except when the proof is specifically requested.

To invent the inductive proof, if you don't see it right off then try showing specific cases for practice, such as P(2) ⇒ P(3) and P(3) ⇒ P(4). Then adapt your reasoning to the full inductive step with n in place of any specific integer.

p. 50, E3: Since n is not prime, we have $n = ab$, where a and b are both integers > 1. If both
$a > \sqrt{n}$ and
$b > \sqrt{n}$

[1] Actually P(0) is technically true also. Since an "empty product" has value 1, P(0) says that if $p|1$ then p divides some a_i. Obviously $p|1$ can't be true, but this is OK: In logic, starting from a false premise you can prove anything, including another false statement such as that p divides some a_i when there aren't any. Let's not be concerned with this.

then multiplying we get $ab > \sqrt{n}\sqrt{n}$, or in other words, $n > n$, which is a contradiction. Therefore one of a and b must be $\leq \sqrt{n}$, say $a \leq \sqrt{n}$. Let p be a prime factor of a; then $p \leq a \leq \sqrt{n}$ and also p is a prime factor of n, as required.

p. 52, E7: Let $a = 2^7 3^2 4^5 5^6 6^5 = 2^7 3^2 (2^2)^5 5^6 (2 \cdot 3)^5 = 2^{22} 3^7 5^6$ and similarly let $b = 2^4 3^5 4^3 5^3 6^7 = \cdots = 2^{17} 3^{12} 5^3$. Then $\gcd(a, b) = 2^{17} 3^7 5^3$, by taking the minimum exponent of each prime involved.

Notes: (1) It's OK to leave the answer in factored form unless the problem says to give an explicit integer as the answer. (2) It might be tempting to write the answer in the form $2^? 3^? 4^? 5^? 6^?$ again but there is more than one way to do this—not surprisingly, since we wouldn't be using a factorization into *primes*.

p. 52, E13: Notice the intuitive idea of this problem: a and m have some prime factors in common giving $\gcd(a, b) = d$, while b and m, being coprime, have no prime factors in common, so ab and m have the same prime factors in common as a and m, still giving d as their gcd.

To say this in detail requires inventing some notation. Since the issue is primes involved in m versus primes not involved in m, let $p_1, \ldots, p_k$ be the distinct prime factors of m and let $p_{k+1}, .., p_n$ be whatever additional distinct primes are involved in a and b. Since m and b are coprime, all the prime factors of b are in this second group. Let $d' = \gcd(ab, m)$. Then we can write "parallel" prime factorizations for all the relevant quantities, with suitable exponents; I'll put first the factorizations and then just a table of exponents for clarity. See just below for explanations of the letters.

$$\begin{array}{ccccccc}
m & = & p_1^{e_1} & \ldots & p_k^{e_k} & p_{k+1}^{0} & \ldots & p_n^{0} \\
a & = & p_1^{f_1} & \ldots & p_k^{f_k} & p_{k+1}^{f_{k+1}} & \ldots & p_n^{f_n} \\
b & = & p_1^{0} & \ldots & p_k^{0} & p_{k+1}^{g_{k+1}} & \ldots & p_n^{g_n} \\
ab & = & p_1^{f_1+0} & \ldots & p_k^{f_k+0} & p_{k+1}^{f_{k+1}+g_{k+1}} & \ldots & p_n^{f_n+g_n} \\
d & = & p_1^{h_1} & \ldots & p_k^{h_k} & p_{k+1}^{0} & \ldots & p_n^{0} \\
d' & = & p_1^{h'_1} & \ldots & p_k^{h'_k} & p_{k+1}^{0} & \ldots & p_n^{0}
\end{array}$$

$$\begin{array}{cccccccc}
m & : & e_1 & \ldots & e_k & 0 & \ldots & 0 \\
a & : & f_1 & \ldots & f_k & f_{k+1} & .:. & f_n \\
b & : & 0 & \ldots & 0 & g_{k+1} & .:. & g_n \\
ab & := & f_1 + 0 & \ldots & f_k + 0 & f_{k+1} + g_{k+1} & \ldots & f_n + g_n \\
d & : & h_1 & \ldots & h_k & 0 & \ldots & 0 \\
d' & : & h'_1 & \ldots & h'_k & 0 & \ldots & 0
\end{array}$$

Here for $i \leq k$ we have $h_i = \min(e_i, f_i) = h'_i$ and for $i > k$ the exponent of p_i is 0 for both d and d', since $0 = \min(0, f_i) = \min(0, f_i + g_i)$. □

(It may be that there is also a solution using Bezout instead of prime factorizations, but I don't see it.)

p. 55, E1: In advance, notice that any odd number is of either the form $4n + 1$ or the form $4n - 1$, for some n, i.e., is congruent to 1 or 3 $\pmod 4$.

Following the idea of Euclid's proof, suppose that there are only finitely many primes of the form $4n-1$, say $p_1, \ldots, p_r$. As suggested, let $a = 4p_1p_2 \ldots p_r - 1$. For each i, since $p_i | a + 1$, p_i does *not* divide a. Therefore a is a product[2] of primes *not* among the p_i. Since a is odd, the prime 2 is not one of its factors, so its factors must all be of the form $4n + 1$ for various values of n. Why is this bad? Think modulo 4: A product of factors each $\equiv 1 \pmod 4$ must be $\equiv 1 \pmod 4$, while $a \equiv -1 \pmod 4$, so we have a contradiction. Therefore there must be infinitely many primes of the form $4n - 1$.

p. 65, E3: This is just asking for remainders after dividing by the modulus. Therefore the answers are 0, 6, 31, 6. (For modulus 9, you now know how to use the fact that positive integer is congruent $\pmod 9$ to the sum of its digits.)

p. 65, E5: (i) $13|1950$, so the numbers are 1951, 1964, 1977, 1990.

(ii) $40|200$, so add 200 to 1776; there isn't room for more between 1950 and 2000, so the only answer number is 1976.

(iii) 1959, 1974, 1989.

p. 67, E5: Use induction. The statement is trivially true for $n = 0$. If we know that $6 \cdot 4^n \equiv 6 \pmod 9$, multiply both sides by 6 to get $6 \cdot 4^{n+1} \equiv 4 \cdot 6 = 24 \equiv 6 \pmod 9$, which verifies the case of $n + 1$ in place of n. Therefore the statement is true for all n by induction. □

(This way of phrasing induction was a little less formal than an answer above that defined P(n) and then talked about P(k) and P($k+1$), but it's the same method.)

p. 67, E6: (i) Solution #1: Starting from $5 \equiv 5$ (mod 7), keep squaring and simplifying to get the residue of 5 to each power-of-2 power: $5^2 = 25 \equiv 4$ (mod 7), $5^4 \equiv 16 \equiv 2 \pmod 7$, $5^8 \equiv 4 \pmod 7$, $5^{16} \equiv 16 \equiv 2 \pmod 7$. The exponent $18 = 16 + 2$, so we multiply the two relevant congruences, getting

[2] Here a itself could be prime, in which case the "product" would have just one factor.

$5^{18} = 5^2 \cdot 5^16 \equiv 4 \cdot 2 = 8 \equiv 1 \pmod{7}$. (Notice that writing 18 as 16 + 2 is really the same as expressing 18 in binary.)

Solution #2: The same as #1, except replace 5 by -2 everywhere, which makes the arithmetic easier.

Solution #3: Since 7 is prime, by Fermat's Little Theorem we have $5^6 \equiv 1 \pmod{7}$. Now cube both sides to get $5^{18} \equiv 1 \pmod{7}$. (This is the easiest method, but it comes after this section in the text. No doubt the author made the problem up this way.)

(ii) Solution #1 in outline: $68 \equiv 3 \pmod{13}$, so $68^{105} \equiv 3^{105} \pmod{13}$. Also by thinking of 105 in binary we have $105 = 64 + 32 + 8 + 1$, so we can use successive squaring and then put some powers together to make 3^{105}. So we find $3^2 = 9 \equiv -4$ (mod 1)3, $3^4 \equiv (-4)^2 = 16 \equiv 3 \pmod{13}$, $3^8 \equiv 3^2 = 9 \pmod{13}$, etc.

Solution #2: As in #1, replace 68 by 3. By Little Fermat, $3^{12} \equiv 1 \pmod{13}$, so we also get residue 1 for any power that is a multiple of 12, since $3^{12k} \equiv 1^k = 1$. Also $105 = 8 \cdot 12 + 9$. Therefore $3^{105} \equiv 3^9 \pmod{13}$. Also $9 = 8 + 1$, so using powers found in Solution #1, we have $3^9 = 3^8 \cdot 3 \equiv 9 \cdot 3 = 27 \equiv 1 \pmod{13}$. To summarize:

$68^{105} \equiv 3^{105} = 3^{8 \cdot 12 + 9} = (3^{12})^8 3^9 \equiv 3^9 \equiv 1 \pmod{13}$.

Solution #3: In the previous solution, notice that $3^3 = 27 \equiv 1 \pmod{13}$. So 3 to any power that is a multiple of 3 is $\equiv 1 \pmod{13}$. Notice that 105 *is* a multiple of 3, so $68^{105} \equiv 3^{105} = 3^{3 \cdot 35} = (3^3)^{35} \equiv 1^{35} = 1 \pmod{13}$. (Probably this is how the author made up the problem—He started by thinking about 13 for the modulus and noticed that 27 works nicely.)

(iii) Notice that 6 and 12 have the same prime factors, so some power of 6 is going to have high enough exponents to be divisible by 12—in fact, 6^2 and higher powers are divisible by 12, so $6^{47} \equiv 0 \pmod{12}$.

p. 74, E5: Running Euclid's algorithm on 313 and 453, we get successive numbers 453, 313, 140, 33, 8, 1 (and 0). Making linear equations in tabular form, starting with ones that are obvious and subtracting the appropriate multiple of each equation from the preceding, we get the following (in which the quotients 1, 2, 4, 4 don't show but are used):

$$\begin{array}{rcrcr}
453 & = & 1 \cdot 453 & + & 0 \cdot 313 \\
313 & = & 0 \cdot 453 & + & 1 \cdot 313 \\
140 & = & 1 \cdot 453 & + & -1 \cdot 313 \\
33 & = & -2 \cdot 453 & + & 3 \cdot 313 \\
8 & = & 9 \cdot 453 & + & -13 \cdot 313 \\
1 & = & -38 \cdot 453 & + & 55 \cdot 313
\end{array}$$

This checks arithmetically. So $313x \equiv 1$ for $x = 55$.

Actually, we could write all this with congruences mod 453 and so omit the "453" column, but let's not.

p. 74, E6: Running Euclid's algorithm on 215 and 7, we get successive numbers 215, 7, 5, 2, 1 (and 0). As in the preceding problem, we get

$$\begin{array}{rcrcr} 215 & = & 1 \cdot 215 & + & 0 \cdot 7 \\ 7 & = & 0 \cdot 215 & + & 1 \cdot 7 \\ 5 & = & 1 \cdot 215 & + & -30 \cdot 7 \\ 2 & = & -1 \cdot 215 & + & 31 \cdot 7 \\ 1 & = & 3 \cdot 215 & + & -92 \cdot 7 \end{array}$$

So $7x \equiv 1 \pmod{215}$ for $x = -92 \equiv 123 \pmod{215}$.

Multiplying through by 13 we get $7x \equiv 13 \pmod{215}$ for $x = 13 \cdot 123 = 1599 \equiv 94 \pmod{215}$.

D-1: (a) The dots in row p (counting from 0), except at the ends.

(b) Because each dot is the sum of the two just above it and because congruences are compatible with addition, working $\pmod{p}$ wherever we have two 0's (red dots) beside each other the one just below is also 0 (red). So as we go down we can fill in a red triangle. In a row such as row p where the residues $\pmod{p}$ are 1, 0, ... , 0, 1, the next row will have some consecutive entries $1+0$ (white), then red for a while, and then $0+1$ (white again). The same is true for each successive row, but the number of 0's in the middle decreases by 1 each time so we get a red triangle bordered by white.

(c) Evidently, if p is prime then $p | \binom{kp}{i}$ except possibly when $p|k$.

(d) Evidently for each power p^k there is a red triangle starting in that row and going all the way across that row except for the ends, so $p | \binom{p^k}{i}$ for $0 < i < p^k$.

D-2: [with the correction that the first paragraph gives $\pi(10^8)$, not $\pi(10^9)$]

(a) $\pi(100) = 25$, just by counting the asterisks in the first line of the first block in the prime-occurrence handout.

(b) The block of 1000 starting with 10^6 has 75 primes, while the density prediction gives $1000/\log(10^6) = 1000/(6 \log(10)) \approx 72.38$, so there are a few more primes than predicted.

The block starting at 10^{100} has two primes, while the density prediction gives $1000/\log(10^{100}) = 1000/(100 \log(10)) \approx 4.34$, so there are not quite as many primes as predicted.

(c) [for 10^8] $\pi(10^8) = 5761455$ (according to the first paragraph of the problem as corrected), while $(10^8)/\log(10^8) = (10^8)/(8\log(10)) \approx 5428681$. So for $n = 10^8$, the ratio of $\pi(n)$ to $n/\log n$ is $5761455/5428681 \approx 1.0613$, off by about 6%.

(d) From the figures given,

$$|\pi(10^{16}) - Li(10^{16})| \approx |279238341033925 - 279238344248557| = 3214632,$$

which does have about half as many digits as 10^{16} (or fewer).

Notes: (1) "Half as many digits" really refers to the square root of n. (2) While the error looks large, with seven digits, it is less than one part in a hundred million compared to n, which is pretty accurate! (3) The idea of integrating a density to get a total amount may be familiar from density problems in calculus.