Solutions to Assignment #6

p. 133, Ex. 10: By the definition of characteristic, $1+1+\cdots+1$ (p times) $= 0$. Then for any a in F, $a(1+1+\cdots+1)$ (p times) $= a0 = 0$. By the distributive law (extended by induction to more terms), this is the same as $a+a+\cdots+a$ (p times) $= 0$.

Note: The same kind of calculation applies in a vector space V over F: By the property $(r+s)v = rv+sv$, extended by induction to the property $(r_1+\cdots+r_k)v = r_1v+\cdots+r_kv$, we have $(1+1+\cdots+1)v = 0v = \mathbf{0}$ (the zero vector) and also $(1+1+\cdots+1)v = v+v+\cdots+v$, so $v+v+\cdots+v = \mathbf{0}$, where each sum mentioned has p terms.

p. 200, Ex. 9: Notice that these are examples in which the moduli are *not* coprime.

In these solutions, a couple of times we'll need the principle that if $x \equiv a \pmod m$ then $x \equiv a$ modulo any divisor of m. For example, $43 \equiv 13 \pmod{10}$ so $43 \equiv 13 \pmod 5$ as well ince $5|10$.

For **(i)**: We are to solve $\begin{cases} x \equiv 11 \pmod{15} \\ x \equiv 8 \pmod{18} \\ x \equiv 6 \pmod{10} \end{cases}$. The solution, if any, will be unique modulo the lcm of the three moduli, which is 90.

First let's solve the first two, by trying to find u, t with $\begin{cases} x = 15u + 11 \\ x = 18t + 8 \end{cases}$. Subtracting gives $15u + 11 - 18t - 8 = 0$ so $15u - 18t = 8 - 11 = -3$ as in (3) on p. 199. Since $\gcd(15,18) = 3$ and $3 \mid -3$, this is possible to solve. The simplest way is to divide through by the gcd, giving $5u - 6t = -1$, or $-5u + 6t = 1$. This is now "coprime Bezout"; we can solve it by eye using $u = 1, t = 1$. Then $x = 15 \cdot 1 + 11 = 26$ solves the first two equations, modulo $\operatorname{lcm}(15,18) = 90$.

Now let's solve $\begin{cases} x \equiv 26 \pmod{90} \\ x \equiv 6 \pmod{10} \end{cases}$. We could use the same method as in the preceding paragraph—but instead, notice that one modulus divides the other, so if there is any solution, $x \equiv 26 \pmod{90}$ is it. And yes, this x does solve the second congruence. To summarize: The original system of simultaneous congruences has solution $x \equiv 26 \pmod{90}$.

For **(ii)**: We are to solve $\begin{cases} x \equiv 6 \pmod{12} \\ x \equiv 3 \pmod{15} \\ x \equiv 18 \pmod{20} \end{cases}$. The solution, if any, will be unique modulo the lcm of the three moduli, which is 60.

First let's solve the first two, by trying to find u, t with $\begin{cases} x = & 12u & + & 6 \\ x = & 15t & + & 3 \end{cases}$. Subtracting gives $12u + 6 - 15t - 3 = 0$ so $12u - 15t = 3 - 6 = -3$ as in (3) on p. 199. Since $\gcd(12, 15) = 3$ and $3 \mid -3$, this is possible to solve. Dividing through by the gcd gives $4u - 5t = -1$, or $-4u + 5t = 1$. We can solve this by eye using $u = 1, t = 1$. Then $x = 12 \cdot 1 + 6 = 18$ solves the first two equations, modulo $\text{lcm}(12, 15) = 60$. Again the third modulus already divides 60, and the same solution works, so the answer for the original system is $x \equiv 18 \pmod{60}$.

For **(iii)**: We are to solve $\begin{cases} x \equiv & -5 & \pmod{21} \\ x \equiv & 1 & \pmod{15} \\ x \equiv & 6 & \pmod{35} \end{cases}$. The solution, if any, will be unique modulo the lcm of the three moduli, which is 105. (Notice that the author made up the problem by choosing primes $3, 5, 7$ and using products of them two at a time for the moduli.)

First let's solve the first two, by trying to find u, t with $\begin{cases} x = & 21u & -5 \\ x = & 15t & +1 \end{cases}$. Subtracting gives $21u - 5 - 15t - 1 = 0$ so $21u - 15t = 1 + 5 = 6$ as in (3) on p. 199. Since $\gcd(21, 15) = 3$ and $3 \mid 6$, this is possible to solve. Dividing through by the gcd gives $7u - 5t = 2$. We can solve this by eye using $u = 1, t = 1$. Then $x = 21 \cdot 1 - 5 = 16$ solves the first two equations, modulo $\text{lcm}(21, 15) = 105$. Again the third modulus already divides 105, but this time the third congruence $x \equiv 6 \pmod{35}$ is not compatible with the solution to the first two. So the original system has no solution.

(To see more clearly why there is no solution, look at the first and third congruences. Since 7 divides both moduli, any solution x must have $\begin{cases} x \equiv & -5 & \pmod{7} \\ x \equiv & 6 & \pmod{7} \end{cases}$, which says x is congruent to both 2 and 6 $\pmod{7}$, an impossibility.)

For **(iv)**: We are to solve $\begin{cases} x \equiv & 2 & \pmod{8} \\ x \equiv & 3 & \pmod{9} \\ x \equiv & 4 & \pmod{12} \end{cases}$. The solution, if any, will be unique modulo the lcm of the three moduli, which is 72.

First let's solve the first two, by trying to find u, t with $\begin{cases} x = & 8u & + & 2 \\ x = & 9t & + & 3 \end{cases}$. The moduli are coprime, so we could use the "basis method" of solving with constants 1,0 and 0,1 first, but instead let's stick with the non-coprime method: Subtracting gives $8u + 2 - 9t - 3 = 0$ so $8u - 9t = 3 - 2 = 1$ as in (3) on p. 199. As mentioned, the moduli are coprime, so we don't need to divide through by the gcd. Solve by eye using $u = -1, t = -1$. Then $x = 8(-1) + 2 = -6$ solves the first two equations, modulo $\text{lcm}(8, 9) = 72$.

Again the third modulus already divides 72 and the solution $x = 6$ fails, so the original problem has no solution.

(To see this more clearly, notice that the second and third congruences imply congruences modulo the gcd of 9 and 12, which is 3; they say $x \equiv 3 \equiv 0 \pmod 3$ and $x \equiv 4 \equiv 1 \pmod 3$, so these two congruences contradict each other.)

p. 201, Ex. 15: The goal of the problem is to give some restrictive congruence conditions on safeprimes, so if a computer is trying to find safeprimes for RSA it can run this preliminary test before trying to see if q and $p = 2q + 1$ are both prime. (RSA doesn't require safeprimes but it's better to use them.)

In each part, it's best to focus on q first, since then we get congruence information for $p = 2q + 1$ as well. Also, notice that neither p nor q can be congruent to 0 modulo 2, 3, or 5, since the only primes of that description *are* 2, 3, and 5, and p and q are specified to be larger than that. Therefore both p and q are congruent to *nonzero* remainders modulo 2, 3, and 5.

Important: Since congruences are compatible with addition and multiplication, knowing $q \equiv c$ modulo some m we know $p = 2q + 1 \equiv 2c + 1 \pmod m$. In each part we can use this fact to make a table of possibilities. Then we avoid any cases where q or p is congruent to 0. For modulus 4 we also have to think modulo 2.

(i)

$q \pmod 3$	0	1	2
$p \pmod 3$	1	0	2

, so $p \equiv 2 \pmod 3$ is the only possibility.

(ii)

$q \pmod 2$	0	1	0	1
$q \pmod 4$	0	1	2	3
$p \pmod 4$	1	3	1	3

, so $p \equiv 3 \pmod 4$ is the only possibility.

(iii)

$q \pmod 5$	0	1	2	3	4
$p \pmod 5$	1	3	0	2	4

, so $p \equiv 2, 3, \text{ or } 4 \pmod 5$.

(iv) For each of the choices $p \equiv 2, 3, \text{ or } 4 \pmod 5$ in (iii), we have three simultaneous congruences, with coprime moduli. Let's use the "basis method", since after doing groundwork we can put any constants on the right.

Solving $x_1 \equiv 1 \pmod 3$, $x_1 \equiv 0 \pmod 4$, $x_1 \equiv 0 \pmod 5$ is the same as $x_1 \equiv 1 \pmod 3$ and $x_1 \equiv 0 \pmod{20}$. Thinking of multiples of 20 we see that a solution is $x_1 = 40$. Solving $x_2 \equiv 0 \pmod 3$, $x_2 \equiv 1 \pmod 4$, $x_2 \equiv 0 \pmod 5$ is the same as $x_2 \equiv 1 \pmod 4$ and $x_2 \equiv 0 \pmod{15}$; thinking of multiples of 15 we see that $x_2 = 45$ is a solution. Solving $x_3 \equiv 0 \pmod 3$, $x_3 \equiv 0 \pmod 4$, $x_3 \equiv 1 \pmod 5$ is the same as solving $x_3 \equiv 1 \pmod 5$ and $x_3 \equiv 0 \pmod{12}$; thinking of multiples of 12 we see that $x_3 = 36$ is a solution. Then a solution to the original problem is $x \equiv 2 \cdot 40 + 3 \cdot 45 + k \cdot 36 \pmod{60}$, where $k = 2$, 3, or 4; reducing mod 60 in each case we get possibilities

$x \equiv 80 + 135 + 72 \equiv 47 \pmod{60}$, $x \equiv 80 + 135 + 108 \equiv 23 \pmod{60}$, and $x \equiv 80 + 135 + 144 \equiv 59 \equiv -1 \pmod{60}$.

This is interesting; of each 60 integers from 20 on, at most three can be safeprimes.

(v) Examine 23, 47, 59, (and adding 60's) 83, 107, 119, 143, 167, 179, 203, 227, 239, ... You can check primeness using the calculator on the class home page. Here 119, 143, 203, and 239 are not prime. (And 143 ought to sound suspicious anyway since it's a square minus 1). Subtracting 1 and dividing by 2 to get q, we get no additional failures. Answer: 47, 59, 83, 107, 167, 179 (and 203, 227).

p. 203, Ex. 3: In $R \times S$ we have $(1,0) \cdot (0,1) = (0,0)$ (the zero element of $R \times S$). Even if R and S don't have a "1" we can take any nonzero elements r in R and s in S and use the example $(r,0) \cdot (0,s) = (0,0)$.

p. 206, Ex. 1: Whenever you see a congruence with a modulus that isn't prime or a prime power, you should think of using the Chinese Remainder Theorem to patch together congruences using moduli that are coprime factors of the original modulus.

In this problem, each solution of $x^2 \equiv 1 \pmod{35}$ is equivalent to finding a solution $\pmod 5$ and a solution $\pmod 7$. Now $x^2 \equiv 1 \pmod 5$ has solutions $x \equiv \pm 1 \pmod 5$ (or 1 and 4) , while $x^2 \equiv 1 \pmod 7$ has solutions $x \equiv \pm 1 \pmod 7$. Now we need to put these together in each possible way:

$x \equiv 1 \pmod 5$ and $x \equiv 1 \pmod 7$ has the obvious solution $x \equiv 1 \pmod{35}$.

Similarly, $x \equiv -1 \pmod 5$ and $x \equiv -1 \pmod 7$ has the obvious solution $x \equiv -1 \pmod{35}$, or $x \equiv 34 \pmod{35}$.

More interesting are the "mixed" solutions:

$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv -1 \pmod 7 \end{cases}$, which we can solve by the "basis" method or just by examining the list of solutions to one congruence and trying them in the other. Taking the second, we try $x = 6, 13, 20, \ldots$, but right off we notice that $x = 6$ works in the first congruence, so The answer is $x \equiv 6 \pmod{35}$. (This is logical: $35 = 5 \cdot 7 = (6+1)(6-1) = 6^2 - 1$, so $6^2 \equiv 1 \pmod{35}$.)

For $\begin{cases} x \equiv -1 \pmod 5 \\ x \equiv 1 \pmod 7 \end{cases}$, we could solve it from scratch, but it is faster to observe that $-1, 1$ are negatives of the preceding simultaneous congruences, so $x \equiv -6 \pmod{35}$ is the answer, or equivalently, $x \equiv 29 \pmod{35}$.

H-1: If the order is k, so that $a^k = 1$ is the first repeat, then $1, a, a^2, \ldots, a^{k-1}$

is a list of k elements. These elements are distinct, because as we saw in lecture, the first repeated power of a must equal 1 if a is a unit.

H-3: (i) In $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, if $p \not| a$ then Little Fermat says $a^{p-1} = 1$ so multiplying through we get $a^p = a$. If $p \mid a$ then $a^p \equiv 0 \pmod{p}$ and $a \equiv 0 \pmod{p}$ so $a^p = a$.

(ii) This problem was corrected to be done only for the cases where a is a unit $\pmod{m}$ or else $m \mid a$. In those cases the solution is the same as (i), giving $a^{\phi(m)} = a$.

But is $a^{\phi(m)} = a$ always true for all a? If m is prime then it is true by (i). The next case to try is where m is a prime power. The simplest example is $m = 4$ so $\phi(m) = 4 - 2 = 2$. Does $a^2 \equiv a \pmod{4}$ for $a = 0, 1, 2, 3$? No; this fails for $a = 2$. So (ii) is not correct for m and a in general.

H-4: As corrected, this problem says that if there is a generator g then there are $\phi(\phi(m))$ generators in all. This is true because we know that the order of g is $\phi(m)$ and we also know that g^i is a generator when i is coprime to the order.

For primes this says the number of generators is $\phi(p-1)$.

An example where m is not prime is $m = 22$: $\phi(22) = \phi(2)\phi(11) = 1 \cdot 10 = 10$; the ten units in $\mathbb{Z}_{22}$ are $1, 3, 5, 7, 9, 13, 15, 17, 19, 21$. It turns out that 3 and 5 are not generators, but 7 is a generator since its powers are

i	0	1	2	3	4	5	6	7	8	9
7^i	1	7	5	13	3	21	15	17	9	19

(and $7^{10} = 1$ again by Euler). The generators are those power 7^i for which i is coprime to 10, namely $i = 1, 3, 7, 9$. So the generators are $7, 13, 17, 19$.

H-5: As suggested, let $b = a^{\frac{p-1}{2}}$. Then $b^2 = a^{p-1} = 1$ by Fermat's Little Theorem since a is nonzero. Solving as in high-school algebra, we have $b^2 = 1$, $b^2 - 1 = 0$, $(b+1)(b-1) = 0$, so one factor or the other is 0, giving $b = -1$ or $b = 1$. Notice that if $p = 2$ these are the same and there is just one solution!

H-6: (i) Let the prime factorization of n be $n = p_1^{e_1} \ldots p_k^{e_k}$. Then $d = p_1^{f_1} \ldots p_k^{f_k}$ with $f_i \leq e_i$ for each i. Since $d < n$, we have a strong inequality $f_i < e_i$ for some i, in which case $d \mid p_1^{e_1} \ldots p_{i-1}^{e_{i-1}} p_i^{e_i - 1} p_{i+1}^{e_{i+1}} \ldots p_k^{e_k}$, or in other words, $d \mid \frac{n}{q}$ with $q = p_i$.

(ii) In this problem a is supposed to be nonzero. This method really contains three ideas. Let's illustrate them for $p = 101$:

(1) The order of any nonzero element a in $\mathbb{Z}_p$ divides $p-1=100$, so in testing whether powers of a return to 1 too soon for a to be a generator, you can just test exponents dividing 100, here $a^2, a^4, a^5, a^{10}, a^{20}, a^{25}, a^{50}$.

(2) If you test this list of powers going right to left, you are able to skip some cases. Start by testing whether $a^{50}=1$. If this is true, then a is not a generator and you are done. If instead $a^{50}\neq 1$, then none of a^2, a^5, a^{10} can be 1, since a^{50} is a power of each of these.

(3) The exponents that you *can't* skip—the ones that don't divide larger exponents—are the ones that are 100 divided by a prime, namely $100/2=50$ and $100/5=20$.

Now the official reasoning:

For the "$\Rightarrow$" direction of the "if and only if": Suppose a is not a generator. For any nonzero a in $\mathbb{Z}_p$ we have $a^{p-1}=1$, so the order of a divides $p-1$. If the order of a were equal to $p-1$ then a would be a generator, which it isn't. Then by (i) the order of a divides $\frac{p-1}{q}$ for some prime factor q of $p-1$, as claimed; in other words, $\frac{p-1}{q}$ is a multiple of the order of a. The multiples of the order are the integers j with $a^j=1$, so $a^{\frac{p-1}{q}}=1$.

For the "$\Leftarrow$" direction: Since $a^{\frac{p-1}{q}}=1$, the list of powers of a returns to 1 too soon for a to generate the $p-1$ units of $\mathbb{Z}_p$.

H-7: The first prime past 10 million is 10,000,019, either from trying candidates in the home-page calculator or by looking at the handout showing primes in blocks of integers. Of course if you're trying candidates, just try odd ones not ending in 5, and you can also skip ones where the sum of the digits is divisible by 3.

For testing generators, factor $p-1=10000018=2\cdot 7\cdot 7\cdot 67\cdot 1523$ using the home-page factorizer. Then using the home-page modular-power calculator, try candidates for a generator. It is handy to type in the powers as 10000018/2, 10000018/7, etc. We find $2^{10000018/7}=1$, $3^{10000018/2}=1$, and $5^{10000018/2}=1$, so 2, 3, and 5 don't work, but $6^{10000018/2}=-1$, $6^{10000018/7}=$ nonzero, $6^{10000018/67}=$ nonzero, $6^{10000018/1523}=$ nonzero, so by H-6, 6 must be a generator.

In this list the candidate 4 was skipped, since the powers of 2 do not include all nonzero elements and the powers of 4 are among the powers of 2.

I-1: (a) α is a generator since its powers are $1, \alpha, \alpha^2=1+\alpha$, and $\alpha+1$ is also a generator since its powers are $1, \alpha+1, \alpha^2+1=\alpha$. This answer could be

expected: There are three units, so every element has order 1 (the element 1 only) or 3 (a generator).

(b) No, $\mathbb{F}_4$ and $\mathbb{Z}/4\mathbb{Z}$ are not isomorphic. They are different from one another in many respects that would be preserved by an isomorphism: $\mathbb{F}_4$ has characteristic 2 while in $\mathbb{Z}/4\mathbb{Z}$ we have $1+1 \neq 0$; $\mathbb{F}_4$ is a field while in $\mathbb{Z}/4\mathbb{Z}$, the element 2 is not a unit (since $2 \cdot 2 = 0$); $\mathbb{F}_4$ has three units while $\mathbb{Z}/4\mathbb{Z}$ has two; and so on.

(c) $x^2 + x + 1$ has no root in $\mathbb{F}_2$, but α is a root in $\mathbb{F}_4$, since $\alpha^2 = 1 + \alpha$ and so $\alpha^2 - 1 - \alpha = 0$, which since the characteristic is 2 becomes $\alpha^2 + \alpha + 1 = 0$.

(d) A good basis of $\mathbb{F}_4$ over $\mathbb{F}_2$ is $1, \alpha$, since each element of $\mathbb{F}_4$ can be written uniquely as $c_0 1 + c_1 \alpha$ with c_0, c_1 being 0 or 1.

I-2: (a)

T_1	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

,

T_α	0	1	α	$1+\alpha$
0	0	α	$1+\alpha$	1
1	1	$1+\alpha$	α	0
α	α	0	1	$1+\alpha$
$1+\alpha$	$1+\alpha$	1	0	α

$T_{1+\alpha}$	0	1	α	$1+\alpha$
0	0	$1+\alpha$	1	α
1	1	α	0	$1+\alpha$
α	α	1	$1+\alpha$	0
$1+\alpha$	$1+\alpha$	0	α	1

(b) As stated, let $(T_r)_{ij} = i + rj$ for r, i, j in some field F and $r \neq 0$.

To show that the entries in row i are distinct (for every i), we must show that $j \neq j' \Rightarrow (T_r)_{ij} \neq (T_r)_{ij'}$, or equivalently[1], that $(T_r)_{ij} = (T_r)_{ij'} \Rightarrow j = j'$, which is the same as saying $i + rj = i + rj' \Rightarrow j = j'$. This last statement does hold, because we can cancel i additively (because of additive inverses in a ring) and then cancel r multiplicatively (because nonzero elements of fields have multiplicative inverses), getting $j = j'$.

To show that the entries in column j are distinct (for every j), we must show that $i \neq i' \Rightarrow (T_r)_{ij} \neq (T_r)_{i'j} \Rightarrow i \neq i'$, or equivalently, $(T_r)_{ij} = (T_r)_{i'j} \Rightarrow i = i'$, which is the same as saying $i + rj = i' + rj \Rightarrow i = i'$. This last statement does hold, because we can cancel rj additively.

(c) We must show that if $r \neq s$ then T_r and T_s are orthogonal, meaning that if we lay one on top of the other the pairs we get (from all the positions in a

[1]Recall that for statements, "P $\Rightarrow$ Q" is equivalent to "not Q $\Rightarrow$ not P", the *contrapositive* of P $\Rightarrow$ Q.

table) are distinct. In other words, if i, j and i', j' different locations in the table, then the pair $\langle (T_r)_{ij}, (T_s)_{ij} \rangle$ is not the same as the pair $\langle (T_r)_{i'j'}, (T_s)_{i'j'} \rangle$. Equivalently, if the pairs *are* the same then the positions *are* the same. From the definition of the tables, then, we must show that

$\langle i + rj, i + sj \rangle = \langle i' + rj', i' + sj' \rangle \Rightarrow i = i'$ and $j = j'$.

Equal pairs have equal corresponding entries, so we are starting with the simultaneous equations

$\begin{cases} i + rj = i' + rj' \\ i + sj = i' + sj' \end{cases}$. Subtracting, we get $(r - s)j = (r - s)j'$. We can cancel $r - s$ since it is a nonzero element of the field, so we get $j = j'$. Substituting back into the first equation, we now get $i + rj = i' + rj$, so canceling rj additively gives $i = i'$, and we are done.

Note. Using two orthogonal 4×4 Latin squares for cards, we can arrange to have each number and each suit be different across each row and column and also to have every number-suit pair occur. But if we use all three 4×4 pairwise orthogonal Latin squares, we can add another feature—having four different decks—in such a way that the decks in each row and column are distinct and there is one ace from each deck, one 2 from each deck, etc., and also one heart card from each deck, one diamond card, etc. To do this, let's call the card numbers A, 2, 3, 4, the suits H, D, S, C, and the decks a, b, c, d. Translate T_1 into card numbers, T_α into suits, and $T_{1+\alpha}$ into decks, and lay the three tables on top of one another. For example, in the second table use $0 \mapsto$ H, $1 \mapsto$ D, $\alpha \mapsto$ S, $1 + \alpha \mapsto$ C. We get

A-H-a	2-S-b	3-C-c	4-D-d
2-D-c	A-C-d	4-S-a	3-H-b
3-S-d	4-H-c	A-D-b	2-C-a
4-C-b	3-D-a	2-H-d	A-S-c

Just about everything here is unique. For example, A occurs with d only once. If we had chosen some other matchup between field elements and card numbers or suits or decks, the resulting triples would have the same properties as now.