Math 115, Summer 2012
Homework 2
Solution

NZM a.b.c refers to a problem in our text, 5th edition - these may differ slightly from the problems appearing in other editions, so use the version printed here to be safe).

(1) (NZM 2.1.5) Write a single congruence that is equivalent to the pair of congruences $x \equiv 1 \mod 4$ and $x \equiv 2 \mod 3$.

Solution: The moduli are prime to each other, so we write one congruence in the new modulus which is the product of the two given moduli, namely 12. If $x \equiv 1 \mod 4$, then $x \equiv 1$ or 5 or 9 mod 12. If $x \equiv 2 \mod 3$, then $x \equiv 2$ or 5 or 8 or 11 mod 12. Thus the only possibility mod 12 which reduces to the given two is $x \equiv 5 \mod 12$.

Alt Sol'n with CRT: We've seen that the Chinese Remainder Theorem (which applies since $(4, 3) = 1$) can be expressed as saying that $\mathbb{Z}/4 \times \mathbb{Z}/3 \cong \mathbb{Z}/12$, and under this isomorphism the element $(1, 2)$ maps to $5 \in \mathbb{Z}/12$.

(2) (NZM 2.1.22) Prove that $n^{6k} - 1$ is divisible by 7 if $(n, 7) = 1$. Here k is any positive integer.

Solution: If n is prime to 7, then $n^6 \equiv 1 \mod 7$, hence $n^{6k} \equiv 1 \mod 7$ for any $k \geq 1$. This means $7 | n^{6k} - 1$.

(3) Find an integer a such that $\{a, a^2, a^3, a^4\}$ is a reduced residue system mod 5.

Solution: This is called a primitive root mod 5. $a = 2$ works, as does $a = 3$, but $a = 4$ does not. We will see soon how to count the number of a mod 5 for which this holds.

(4) Find the smallest positive integer x which is congruent to 32^{412} mod 7.

Solution: We use Fermat's little Thm, which says in this case that since 32 is prime to 7, $32^6 \equiv 1 \mod 7$. Since $412 = 68 \cdot 6 + 4$,

$$32^{412} = (32^6)^{68} \cdot 32^4 \equiv 1^{68} \cdot 4^4 = 16^2 \equiv 2^2 = 4 \mod 7$$

(5) (NZM 2.1.33) Show that $\{1^2, 2^2, 3^2, \ldots, m^2\}$ is not a complete residue system mod m if $m > 2$.

Solution: It's not a complete residue system because for any $m > 2$, both 1^2 and $(m-1)^2$ are congruent to 1 mod m. (This fails for $m = 2$ since in this case $1 = m - 1$).

(6) (NZM 2.1.35) If n is a composite positive integer, show that $(n-1)! + 1$ is not a power of n.

Solution: We can prove an even stronger result, which is a converse to Wilson's Theorem, namely if n is composite, $(n-1)! \not\equiv -1 \mod n$. To see this, suppose that n has a prime factor p. Then $p < n - 1$, and thus p appears as a factor in the product $(n-1)!$, which is therefore congruent to zero mod p. Hence it is not congruent to -1 mod p, and so cannot be congruent to -1 mod n, either. Thius shows that $(n-1)! + 1$ is not even a multiple of n, much less a power of it.

(7) (NZM 2.1.40) If m is odd, show that the sum of all the elements of $\mathbb{Z}/m$ is equal to zero.

Solution: The key is that m is odd, so there are an even number of nonzero elements in this ring. They pair up to give zero. More rigorously:

$$\sum_{i=1}^{m} i = (1 + (m-1)) + (2 + (m-2)) + \cdots (m/2 + (m - m/2)) = m + m + \cdots + m \equiv 0 \mod m$$

(8) (NZM 2.1.48) If $r_1, \ldots, r_p$ and $r_1', \ldots, r_p'$ are any two complete residue systems mod p, where p is a prime greater than 2, show that the set $\{r_1r_1', r_2r_2', \ldots, r_pr_p'\}$ is not a complete residue system mod p.

Solution: Suppose that the set $S = \{r_1r_1', r_2r_2', \ldots, r_pr_p'\}$ forms a complete residue system mod p. Exactly one of the r_i is congruent to zero mod p, call it r_j, and exactly one of the r_i' is congruent to zero mod p, call it r_k'. If $j \neq k$, there are two elements of S congruent to zero mod p, so it's not a complete residue system. Since we assumed it was, we must have that $j = k$. Now we might as well reorder S so that $r_1 \equiv r_1' \equiv 0 \mod p$. Then by Wilson's Thm, we have

$$\prod_{i=2}^{p}(r_ir_i') \equiv -1 \mod p$$

but also, splitting the product we have

$$\prod_{i=2}^{p}(r_ir_i') = \prod_{i=2}^{p} r_i \prod_{i=2}^{p} r_i' \equiv (-1)(-1) \equiv 1 \mod p,$$

since each of $\{r_i\}$ and $\{r_i'\}$, with $2 \leq i \leq p$, forms a complete residue system. This is a contradiction, since $-1 \not\equiv 1 \mod p$ unless $p = 2$, and we assumed that $p > 2$.

(9) (NZM 2.2.5d,e) Find all solutions of the congruences $57x \equiv 87 \mod 105$ and $64x \equiv 83 \mod 105$.

Solution: For the first one, we compute $(57, 105) = 3$. Since $3|87$, there is a solution which is unique mod $\frac{105}{3} = 35$. We first divide the congruence through by the gcd, giving

$$19x \equiv 29 \mod 35$$

To find the inverse of 19 mod 35, we use div alg:

$$\begin{aligned} 35 &= 1 \cdot 19 + 16 \\ 19 &= 1 \cdot 16 + 3 \\ 16 &= 5 \cdot 3 + 1 \end{aligned}$$

So

$$1 = 16 - 5 \cdot 3 = 16 - 5(19 - 16) = -5 \cdot 19 + 6 \cdot 16 = -5 \cdot 19 + 6(35 - 19) = 6 \cdot 35 - 11 \cdot 19$$

So reducing this mod 35 shows that -11 is inverse to 19 mod 35. Thus

$$x \equiv -11 \cdot 19x \equiv -11 \cdot 29 = -319 \equiv 31 \mod 35$$

The strategy for the second one is similar, and the answer is $x \equiv 62 \mod 105$.

(10) (NZM 2.3.2) Find all integers x that satisfy all three congruences

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 1 \mod 5 \\ x &\equiv 1 \mod 7. \end{aligned}$$

Solution: After noting that the moduli are relatively prime, we set $m = 3 \cdot 5 \cdot 7 = 105$. We want inverses to $\frac{m}{m_i} \mod m_i$, for $i = 1, 2, 3$.

$$\begin{aligned}
(\frac{m}{m_1})^{-1} &= (\frac{105}{3})^{-1} = 35^{-1} \equiv (-1)^{-1} = -1 \mod 3 \\
(\frac{m}{m_2})^{-1} &= (\frac{105}{5})^{-1} = 21^{-1} \equiv 1^{-1} = 1 \mod 5 \\
(\frac{m}{m_3})^{-1} &= (\frac{105}{7})^{-1} = 15^{-1} \equiv 1^{-1} = 1 \mod 7
\end{aligned}$$

So we set

$$x = 35 \cdot (-1) \cdot 1 + 21 \cdot 1 \cdot 1 + 15 \cdot 1 \cdot 1 = 1 \mod 105$$

This implicitly gives all integer solutions: all others differ from 1 by a multiple of 105, so the solution set is $\{\dots, -104, 1, 106, \dots\}$.

(11) (NZM 2.3.7) Determine whether the congruences $5x \equiv 1 \mod 6$ and $4x \equiv 13 \mod 15$ have a common solution. Find the solutions, if any exist.

Solution: The moduli are not pairwise prime, so we split each modulus into prime power factors and obtain a larger sytem of congruences as follows: $5x \equiv 1 \mod 6$ is equivalent to the two congruences $x \equiv 1 \mod 2$ and $2x \equiv 1 \mod 3$. The other congruence, $4x \equiv 13 \mod 15$, is equivalent to the two $x \equiv 1 \mod 3$ and $4x \equiv 3 \mod 5$. Out of these four new congruences, two are both mod 3, and they are inconsistent: If $x \equiv 1 \mod 3$, then $2x \equiv 2$, not 1,

(12) (NZM 2.3.19) Let $m_1, \dots, m_r$ be relatively prime in pairs. Assuming that each of the congruences $b_i x \equiv a_i \mod m_i$ has a solution, prove that the congruences have a simultaneous solution (i.e., one x that satisfies all congruences at once).

Solution: This is just like the CRT, except now there's a coefficient on each x. But our assumption is that each congruence $b_i x \equiv a_i \mod m_i$ has a solution, which we have seen can happen if and only if $g_i = (b_i, m_i)$ divides a_i. Divide through each congruence by g_i, giving

$$\frac{b_i}{g_i} x \equiv \frac{a_i}{g_i} \mod \frac{m_i}{g_i}$$

All the new moduli $\frac{m_i}{g_i}$ are still pairwise prime, and moreover, the coefficient v is prime to the modulus $\frac{m_i}{g_i}$, so it has a multiplicative inverse mod $\frac{m_i}{g_i}$, call it c_i. Multiplying each of these new congruences by this inverse gives a system of congruences of the form

$$x \equiv \frac{a_i}{g_i} c_i \mod \frac{m_i}{g_i},$$

which have a common solution by the CRT.

(13) (NZM 2.3.37) Let $a_1 = 3$, $a_{i+1} = 3^{a_i}$. Describe this sequence mod 100.

Solution: The first observation to make is that $\phi(100) = \phi(4)\phi(25) = 2 \cdot 20 = 40$, so $3^{40} \equiv 1 \mod 100$ by Euler's Thm. Since our sequence consists of big powers of three, it is natural to find which powers of 3 this is useful for. Since $3^4 = 81 = 2 \cdot 40 + 1$, we note that

$$3^{3^4} \equiv 3 \mod 100$$

To see how to use this, begin to write some a_i: $a_1 = 3$, $a_2 = 3^3 = 27$, $a_3 = 3^{3^3} = 3^{27}$, and this is already to large to calculate unless you've got a good calculator, but continuing on, we have

$$a_4 = 3^{3^{3^3}}$$

We know that $3^{3^4} \equiv 3$, and a_4 is bigger than 3^{3^4}, and they're both powers of 3^3. This means we can write a_4 as some power of 3^{3^4}, namely

$$a_4 = 3^{3^{3^3}} = (3^{3^4})^{3^{3^3-4}}$$

This is maybe clearer if we write it as $3^{3^k} = (3^{3^4})^{3^{k-4}}$, which holds as long as $a > 3$. Now we apply $3^{3^4} \equiv 3$ and get

$$a_4 \equiv 3^{3^{3^3-4}} = 3^{3^{23}}$$

So we were able to reduce $3^{3^{27}}$ to $3^{3^{23}}$. Since 23 is still bigger than 3, we can do the same again (with $k = 23$ in the above) a few more times to get

$$a_4 \equiv 3^{3^{19}} \equiv \cdots \equiv 3^{3^3} \mod 100$$

so actually $a_3 \equiv a_4 \mod 100$. Naturally one hopes that this continues, i.e., all the a_i for $i \geq 3$ are congruent. This is true, and how to prove it? The formula from before,

$$3^{3^k} = (3^{3^4})^{3^{k-4}},$$

which holds for $k > 3$, implies that we can repeatedly subtract 4 from the exponent of 3^3, so if $k \equiv \overline{k} \mod 4$, where $0 \leq \overline{k} < 4$ is the smallest nonegative residue of k mod 4, we have

$$3^{3^k} \equiv 3^{3^{\overline{k}}} \mod 100$$

Now notice that $a_n = 3^{a_{n-1}} = 3^{3^{a_{n-2}}}$, so we can replace a_{n-2} here by its smallest non-negative residue mod 4. But $3^2 \equiv 1 \mod 4$ by Euler, and so $a_n \equiv 3 \mod 4$ for all n. Thus

$$a_n = 3^{a_{n-1}} = 3^{3^{a_{n-2}}} \equiv 3^{3^3} \mod 100$$

for $n \geq 3$ (we need $n \geq 3$ in order to be able to reduce the top exponent mod 4).

(14) Which of the following are ring homomorphisms?

(a) $f \colon \mathbb{Z} \to \mathbb{Z}/2$ given by $f(n) = 0$ if n is even and 1 if n is odd.
Solution: This is a ring map - it is a special case of the "reduction mod m" map $\mathbb{Z} \to \mathbb{Z}/m$ which we discussed in class (here $m = 2$).

(b) $g \colon \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = nx$, where n is some fixed integer.
Solution: This cannot be a ring map unless $n = 1$, since any ring map has to send 1 to 1. When $n = 1$, we just get the identity map, which is a homomorphism.

(c) $E_3 \colon \mathbb{Z}[x] \to \mathbb{Z}$ which sends a polynomial $f(x) \in \mathbb{Z}[x]$ to the integer $f(3)$.
Solution: This is a ring map. Some would call this map "evaluation at 3".

(d) Let $M_2(\mathbb{Z})$ be the set of all 2×2 matrices with integer entries. $h \colon M_2(\mathbb{Z})$ is the trace map, which sends a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $a + d$.
Solution: This is not a ring map - it sends $1 \in M_2(\mathbb{Z})$, which is just the identity matrix, to $2 \in \mathbb{Z}$.

(15) Let $R = \mathbb{Z}[\sqrt{5}]$ be the ring consisting of elements of the form $a + b\sqrt{5}$, where a and b are integers. Let S be the ring consisting of matrices of the form $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$. Prove that R is isomorphic to S.

Solution: First we define a homomorphism $f\colon R \to S$ by the formula

$$f(a+b\sqrt{5}) = \begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$$

To see that this is a homomorphism, we must check:

$$\begin{aligned} f((a+b\sqrt{5})(c+d\sqrt{5})) &= f((ac+5bd)+(ad+bc)\sqrt{5}) \\ &= \begin{pmatrix} ac+5bd & ad+bc \\ 5(ad+bc) & ac+5bd \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ 5b & a \end{pmatrix}\begin{pmatrix} c & d \\ 5d & c \end{pmatrix} \\ &= f(a+b\sqrt{5})f(c+d\sqrt{5}) \end{aligned}$$

So f is multiplicative. The check for additivity is similar.

Finally, the element 1 in the ring R is $1 = 0\sqrt{5}$, and 1 in the ring S is the 2×2 identity matrix. So the check that f sends 1 to 1 is as follows:

$$f(1+0\sqrt{5}) = \begin{pmatrix} 1 & 0 \\ 5 \cdot 0 & 1 \end{pmatrix}$$

Now we have to check that this f is not just a homomorphism, but an isomorphism. This means that it is one-to-one and onto, or equivalently, that it has an inverse. It is easier to check it has an inverse, namely the map $g\colon S \to R$ which sends $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$ to $a+b\sqrt{5}$.

(16) Find all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/12$.

Solution: Any ring map f must send $1 \in \mathbb{Z}$ to $1 \in \mathbb{Z}/12$. For any integer $n \in \mathbb{Z}$, we can write $n = 1+1+\cdots+1$, and applying f gives $f(n) = f(1+\cdots+1) = f(1)+f(1)+\cdots+f(1) = 1+\cdots+1$. This means that for any ring homomorphism out of $\mathbb{Z}$, what it does to any integer n is determined by the property $f(1) = 1$. Thus there is only one map $\mathbb{Z} \to \mathbb{Z}/12$. In fact, the argument shows that there is only one ring map $\mathbb{Z} \to R$ for *any* ring R!.