# Solutions to Homework 6.

March 20, 2013

**Problem** 3**.**

The waking times (in hours after midnight on April 1) differ by multiples of $17 + 8 = 25$ hours. Therefore each time she wakes 1 hour later on the 24 hour cycle and on the 24th day will have risen at each possible hour.

If she stays awake for 18 hours then each time she will wake 2 hours later and will always rise at an even hour. Therefore the conclusion is false.

**Problem** 5**.**

$10 \equiv -1 \bmod 11$. Therefore $10^n \equiv (-1)^n \bmod 11$ and $10^n \equiv 1 \bmod 11$ if $n$ is even and $10^n \equiv -1 \bmod 11$ if $n$ is odd.

$$654321 = 6 \cdot 10^5 + 5 \cdot 10^4 + 4 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10 + 1.$$

Therefore, computing modulo 11 gives

$$654321 \equiv -6 + 5 - 4 + 3 - 2 + 1 \equiv -3 \bmod 11.$$

Hence 8 is the remainder if we divide 654321 by 11.

**Problem** 8**.**

if $k$ is odd then we can write $k = 2l + 1$ for an integer $l$. Then

$$k^2 - 1 = (2l + 1)^2 - 1 = (4l^2 + 4l + 1) - 1 = 4l(l + 1).$$

Now, either $l$ or $l + 1$ is even and so $2|l(l + 1)$ and hence $2 \cdot 4 = 8$ divides $4l(l + 1)$.

**Problem** 11**.**

(a) The relation $R$ is not transitive. For example, $gcd(2,6) = 2 > 1$ and $gcd(6,3) = 3 > 1$ and so $(2,6) \in R$ and $(6,3) \in R$. However $gcd(2,3) = 1$ and so $(2,3) \notin R$.

(b) This is an equivalence relation. To prove this we need to check that the relation is reflexive, symmetric and transitive.

(i) Reflexive. If $x \in \mathbb{R}$ then $x = 2^0 \cdot x$ and so $(x,x) \in R$.

(ii) Symmetric. If $(x,y) \in R$ then $x = 2^n \cdot y$ for some $n \in \mathbb{Z}$. Therefore $y = 2^{-n} \cdot x$ and so $(y,x) \in R$ also.

(iii) Transitive. Suppose that $(x,y) \in R$ and $(y,z) \in R$. Then there exist $m, n \in \mathbb{Z}$ such that $x = 2^m \cdot y$ and $y = 2^n \cdot z$. Multiplying this gives $x = 2^{m+n} \cdot z$ and so $(x,z) \in R$ also as required.

**Problem** 32**.**

Suppose that $\overline{ax} = \overline{b}$, then $ax \equiv b \bmod n$ or $ax = b + kn$ for some $k \in \mathbb{Z}$. But as $d = gcd(a,n)$ divides both $a$ and $n$ it must also divide $b$. Hence there are no solutions unless $d|b$.

Suppose that $d|b$. Then we can write $a = pd$, $b = qd$ and $n = rd$ for some $p, q, r \in \mathbb{Z}$ and we have $ax = b + kn$ for some $k \in \mathbb{Z}$ if and only if $px = q + kr$ for some $k \in \mathbb{Z}$, or in other words $px = q \bmod r$.

Now, as $d = gcd(a,n)$ we must have that $p$ and $r$ are relatively prime. Therefore by Lemma 7.27 this last equation does have a solution $x$, and the solution is unique modulo $r$.

Let $x_0$ be one solution, then the set of all solutions is $\{x \in \mathbb{Z} | x = x_0 + lr \text{ some } l \in \mathbb{Z}\}$. We need to see how many congruence classes these solutions give modulo $n = rd$.

If $l_1 \equiv l_2 \bmod d$ then $x_0 + l_1 r \equiv x_0 + l_2 r \bmod rd = n$ and so there are at most $d$ congruence classes, namely the congruence classes of

$$x_0, x_0 + r, x_0 + 2r, \ldots, x_0 + (d-1)r.$$

Finally we claim that these congruence classes are all different modulo $n = rd$ and so there are exactly $d$ congruence classes.

Suppose $x_0 + ir \equiv x_0 + jr \bmod d$ for some $0 \leq i, j \leq d-1$. Then $(i-j)r \equiv 0 \bmod n$. Dividing by $r$ this says that $i - j \equiv 0 \bmod d$ and hence $i = j$ and required.

**Problem** 34**.**

We use the Chinese Remainder Theorem with $a_1 = 1$, $a_2 = 3$, $a_3 = 5$ and $n_1 = 7$, $n_2 = 8$, $n_3 = 9$. First we observe that $n_1, n_2, n_3$ are pairwise relatively prime as they have no prime factors in common. Then we set $N = n_1 n_2 n_3$, $N_i = N/n_i$ and get the following table.

| $i$ | $a_i$ | $n_i$ | $N_i$ | $N_i \bmod n_i$ | $y_i$ |
|---|---|---|---|---|---|
| 1 | 1 | 7 | 72 | 2 | 4 |
| 2 | 3 | 8 | 63 | -1 | -3 |
| 3 | 5 | 9 | 56 | 2 | 7 |

Here $y_i$ is a solution to $y_i N_i = a_i \bmod n_i$.

A solution to the problem is given by $x = \sum_i N_i y_i = 72 \cdot 4 - 3 \cdot 63 + 7 \cdot 56 = 491$.

The solution is unique modulo $N = 504$. Therefore the solution with smallest absolute value is $491 - 504 = -13$.

**Problem** 35**.**

The Chinese Remainder Theorem is not directly valid here since 6 and 8 are not relatively prime, 2 is a common factor. However as $x \equiv 3 \bmod 6$ it must be odd and so we set $x = 2k + 1$ and try to solve instead for $k$.

The first equation is $2k + 1 \equiv 3 \bmod 6$ which implies $2k \equiv 2 \bmod 6$ or, dividing by 2, $k \equiv 1 \bmod 3$.

The second equation is $2k + 1 \equiv 4 \bmod 7$ which implies $2k \equiv 3 \bmod 7$. Multiplication by 2 gives a bijection on $\mathbb{Z}_7$ and so the only possibility here is that $k \equiv 5 \bmod 7$.

The third equation is $2k + 1 \equiv 5 \bmod 8$ or $2k \equiv 4 \bmod 8$ which implies $k \equiv 2 \bmod 4$.

We now have three equations to which the C.R.T. is valid.

The corresponding table is

| $i$ | $a_i$ | $n_i$ | $N_i$ | $N_i \bmod n_i$ | $y_i$ |
|---|---|---|---|---|---|
| 1 | 1 | 3 | 28 | 1 | 1 |
| 2 | 5 | 7 | 12 | 5 | 1 |
| 3 | 2 | 4 | 21 | 1 | 2 |

Now we get the solution $k = \sum_i N_i y_i = 28 + 12 + 2 \cdot 21 = 82$, which is unique modulo $N = 84$.

Plugging in the possible values of $x$ are $x = 2k + 1 = 164 + 84l + 1$ for $l \in \mathbb{Z}$. Taking $l = -1$ gives $-3$, so the smallest positive solution is when $l = 0$, which is $x = 164 + 1 = 165$.

*Remark.* Another approach here, as discussed in class, is to consider instead solutions to the equations $x \equiv 0 \bmod 3$, $x \equiv 4 \bmod 7$ and $x \equiv 5 \bmod 8$.

It can easily be shown that solutions to the first set of equations also solve this new system. Therefore the solutions to this new system (which *can* be found using the C.R.T.) will include all solutions to the original and we can check directly that the smallest solution is the one we need.