Math 55 Fall '12
HW 7 Solutions

4.4 #26. To solve $x \equiv 5 \pmod 6$, $x \equiv 3 \pmod{10}$, $x \equiv 8 \pmod{15}$, we'll rewrite these congruences modulo the pairwise relatively prime moduli 2, 3 and 5. By CRT, $x \equiv 5 \pmod 6$ is equivalent to $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$. Similarly, $x \equiv 3 \pmod{10}$ is equivalent to $x \equiv 1 \pmod 2$, $x \equiv 3 \pmod 5$, and $x \equiv 8 \pmod{15}$ is equivalent to $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$. These congruences are consistent with each other (if they had not been, it would mean there is no solution), and reduce to

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5.$$

Using either fundamental solutions or back-substitution we discover that the solution is

$$x \equiv 23 \pmod{30}.$$

4.4 #38 a) By Fermat,

$$3^{302} \equiv 3^2 \equiv 4 \pmod 5$$
$$3^{302} \equiv 3^2 \equiv 2 \pmod 7$$
$$3^{302} \equiv 3^2 \equiv 9 \pmod{11}$$

b) By CRT and part (a), $3^{302} \equiv 9 \pmod{385}$

4.4 #46 We are to show that for all x relatively prime to 1729, we have $x^{1728} \equiv 1 \pmod{1729}$. Now, $1729 = 7 \cdot 13 \cdot 19$, and by Fermat, we have $x^{1728} = x^{6 \cdot 288} \equiv 1 \pmod 7$, $x^{1728} = x^{12 \cdot 144} \equiv 1 \pmod{13}$, $x^{1728} = x^{18 \cdot 96} \equiv 1 \pmod{19}$. Hence, by CRT, $x^{1728} \equiv 1 \pmod{1729}$. This holds for all x not divisible by 7, 13, or 19, i.e. for all x rel. prime to 1729.

Now we'll apply Miller's test with base $x=2$. Since $1728 = 2^6 \cdot 27$, we should calculate $2^{27}, 2^{54}, 2^{108}, \ldots, 2^{1728} \pmod{1729}$:

$2^{27} \equiv 645$, $2^{54} \equiv 645^2 \equiv 1065$, $2^{108} \equiv 1065^2 \equiv 1$,
$2^{216} \equiv 1$, $2^{432} \equiv 1$, $2^{864} \equiv 1$, $2^{1728} \equiv 1$.

Since the sequence

$$645, 1065, 1, 1, 1, 1$$

does not end with $-1, 1, \ldots, 1 \pmod{1729}$ [note $1065 \not\equiv -1 \pmod{1729}$], the number 1729 failed Miller's test, and we see from this that it is not prime, even though it passes Fermat's test (being a Carmichael number).

4.4 #54 "Primitive root" means that 2^{18} is the smallest power $\equiv 1 \pmod{19}$. One way to verify this is calculate all powers $2^0, 2^1, \ldots, 2^{17} \bmod 19$. A more clever way is to observe that if $2^m \equiv 1 \bmod 19$ for some $m < 18$, the smallest such m divides 18, and it follows that we must have $2^k = 1$ for one of the 'maximal' divisors $k = 9$ or $k = 6$ of 18, which have no other divisors of 18 as multiples, except 18 itself. But $2^6 \equiv 64 \equiv 7 \pmod{19}$, and $2^9 \equiv 8 \cdot 7 \equiv 56 \equiv 18 \pmod{19}$. So 2 is a primitive root.

4.6 #26 Using Euclidean algorithm with back substitution, we find $1 = -367 \cdot 17 + 2 \cdot (52 \cdot 60)$, so $d \equiv -367 \equiv 2753 \pmod{52 \cdot 60}$. Thus 2753 is our decryption exponent, and the decryption function is $D(x) = x^{2753} \pmod{3233}$, since $n = 53 \cdot 61 = 3233$. Applying this to each block of the encrypted message, we decrypt to 1816 2008 1717 0411. Note that $2753 = 2^{11} + 2^9 + 2^7 + 2^6 + 1$, for modular exponentiation. Or, since we know the factorization of n, we could use the Chinese Remainder Theorem + Fermat to compute $x^{2753} \pmod{53 \cdot 61}$ from $x^{2753} \equiv x^{49} \pmod{53}$ and $x^{2753} \equiv x^{53} \pmod{61}$. In the character encoding A=00, B=01, etc., 18 16 20 08 17 17 04 11 = SQUIRREL.

Additional Problem

Here is the table of $x_i = f(x_{i-1})$, $y_i = f(f(y_{i-1}))$, $\gcd(y_i - x_i, n)$ where $f(x) = x^2+2 \bmod n$, starting with $x_0 = y_0 = 2$, for $n = 43489$:

i	x_i	y_i	$\gcd(y_i - x_i, n)$
0	2	2	1
1	6	38	1
2	38	3446	1
3	1446	33717	1
4	3446	25740	157

We discovered the factor 157, and the resulting factorization

$n = 157 \cdot 277$