1. Find a solution to the congruence $x^2 - 5x + 39 \equiv 0 \pmod{77}$. (I'll give a few bonus points if you can find additional solutions, and a few more if you can demonstrate you have found all the solutions.)

ANSWER: We need $x^2 - 5x + 4 \equiv 0$ mod 7; two solutions are $x = 1$ and $x = 4$, and since 7 is prime all solutions must be congruent to one of these two modulo 7. Likewise we need $x^2 - 5x + 6 = (x-2)(x-3) \equiv 0$ mod 11, which has just two solutions $x \equiv 2$ and $x \equiv 3$. So by the Chinese Remainder Theorem there will be four solutions modulo 77.

For example if $x \equiv 2$ mod 11 then $x = 2 + 11k$ for some integer k; this is congruent to 1 modulo 7 iff $-3k \equiv -1$ mod 7, which requires $k \equiv 5$ mod 7, and then $x = 2 + 11k \equiv 57$ modulo 77.

In exactly the same way we discover the other three solutions to be the congruence classes of 25, 36, and 46 modulo 77.

2. Find all solutions to the congruence $x^2 \equiv 44 \pmod{43^2}$.

ANSWER: Suppose $x^2 \equiv 44$ modulo 43^2. Then also $x^2 \equiv 44 \equiv 1$ mod 43. Since 43 is prime there can only be two square roots of 1 and they are obviously ± 1. Thus $x = \pm(1 + 43k)$ for some integer k. Since $x^2 \equiv 44$ modulo 43^2, this expands to $1 + 86k \equiv 44$, i.e. $86k \equiv 43$ mod 43^2. Divide by 43 to conclude that $2k \equiv 1$ mod 43, and then multiply by $2^{-1} = 22$ to conclude $k \equiv 22$ mod 43, so that $x \equiv \pm(1 + 43 \cdot 22) = \pm 947$ modulo $43^2 = 1849$.

3. The number $N = 5^9 - 1$ equals 4×488281. Find a proper divisor of 488281.
(Hint: we have discussed the factors of the polynomials $X^n - 1$.)

ANSWER: We know $X^3 - 1$ has $X - 1$ as a factor; use $X = 5^3$ to see N has $124 = 4 \times 31$ as a factor, so that 31 divides $N/4$. (Then $488281/31 = 15751$, which happens to factor as $19 \cdot 829$ but I don't think that's obvious.)

If you only thought to use this generic factorization with $X = 5$ and $n = 9$, then you could still discover

$$488421 = (5^8+5^7+5^6)+(5^5+5^4+5^3)+(5^2+5^1+5^0) = (5^6+6^3+1)(5^2+5+1) = 15751 \cdot 31$$

(In base-5 notation this is simply the observation that $111,111,111_5 = 1,001,001_5 \times 111_5$.)

You could also use Fermat's method of factorization, which is treated in the book but which we discussed little (if at all) in class. If 488281 is a product of two factors $a \cdot b$ (obviously both odd), let $m = (a+b)/2$ be the number in the middle between them and let $d = |m - a| = |m - b|$ be the distance from m to these factors. Then $a = m + d$ and $b = m - d$, and so $488281 = ab = m^2 - d^2$. Fermat's idea was to try values of m, looking to see which make $m^2 - 488281$ a square. Clearly in this case we need m larger than around 700 (actually we should start at $m = 699$); for example if $m = 700$ then $m^2 - 488281 = 1719$ is positive but not a perfect square. Note that $(m+1)^2 - 488281 =$

$(m^2 - 488281) + (2m + 1)$, which means we may quickly compute successive values of $m^2 - 488281$ by adding consecutive odd numbers: when $m = 701$ this difference equals $1719 + 1401 = 3120$ (which is not a square); for the next m it equals $3120 + 1403 = 4523$ (not a square); then come $5928, 7335, 8744, 10155, 11568, 12983$, and finally $14400 = 120^2$ when $m = 709$. So $488281 = 709^2 - 120^2 = 829 \cdot 589$. As it turns out, 829 is prime but 589 can also be factored using the Fermat method: on the very first step we start with $m = 25$ and note that $m^2 - 589 = 36$ is a square, so $589 = 25^2 - 6^2 = 19 \cdot 31$, giving us some additional factors of 488281. I didn't expect anyone to try this method but at least one person did and you are welcome to try it in the future.

4. Show that for every integer n we have $\phi(n^2) = n\phi(n)$. (Here, ϕ is the "Euler phi-function".)

ANSWER: One way to compute $\phi(n^2)$ is as

$$\phi(n^2) = n^2 \cdot \prod_{p|n^2} \left(1 - \frac{1}{p}\right),$$

the product taken over all primes dividing n^2. But those are *the same primes* as the primes dividing n itself, so that $\phi(n^2) = n \cdot n \cdot \prod_{p|n}(1 - \frac{1}{p}) = n \cdot \phi(n)$.

You could also compute $\phi(n^2)$ as the number of integers in the set $S = \{0, 1, \ldots, n^2-1\}$ which are coprime to n^2. First note that we can also describe S as $\{x = an + b \,|\, 0 \leq a, b < n\}$ (by the division algorithm); second note that $x \perp n^2$ iff $x \perp n$, and that $\gcd(x, n) = \gcd(b, n)$. Thus the set of integers we are trying to count is exactly the set

$$\{x = an + b \,|\, 0 \leq a < n \text{ and } b \in T\}$$

where T is the set of integers from 0 to $n - 1$ which are coprime to n. There are n such a and $\phi(n)$ such b, giving $n\phi(n)$ such integers x.

5. Show that if p is a prime and $p \equiv 1 \bmod 4$, then the integer $x = \left(\frac{p-1}{2}\right)!$ satisfies $x^2 \equiv -1 \bmod p$. (Hint: use the theorem that has factorials in it! You might want to consider an example like $p = 13$ to see what's going on.)

ANSWER: By Wilson's theorem, $(p-1)! \equiv -1 \bmod p$. Now, $(p-1)!$ is the product of a total of $p - 1$ terms, half of which multiply out to be x. The other half of the terms are the negatives of these modulo p; pairing each integer $n \leq (p-1)/2$ with its negative shows that the product of these other integers will be congruent to $(-1)^{(p-1)/2} \cdot ((p-1)/2)! = (-1)^{(p-1)/2}x$. So in this way we have rewritten Wilson's Theorem to say $-1 \equiv (-1)^{(p-1)/2}x^2 \bmod p$. Since $p \equiv 1 \bmod 4$, that exponent is even, and we are left with $x^2 \equiv -1 \bmod 4$.

Note that this shows -1 has a square root modulo such primes. It's not hard to show that -1 does NOT have a square root mod p when $p \equiv 3 \bmod 4$; for example, no square is congruent to $-1 \bmod 7$. What the proof above does show for such primes is that $x^2 \equiv +1$, and as you know the only integers whose square is 1 modulo a prime are $+1$ and -1, so we deduce that $x \equiv \pm 1 \bmod p$ whenever $p \equiv 3 \bmod 4$. It is an extremely subtle project to determine which of these primes make $x \equiv 1$ and which make $x \equiv -1$!

EXTRA CREDIT. In our discussion of cryptography we imagined Alice encrypting a message by replacing each integer a with another integer $b \equiv a^d$ modulo N. (You may recall that the values of b, d, and N could be made public to everyone without compromising security!) Bob would then decrypt the message by re-computing a from b; he would do this by computing $a \equiv b^e \bmod N$ for some exponent e that only he could figure out, because only he knew the factorization of N.

Well, here is your chance to play the role of Eve. Suppose Alice and Bob have announced to the world that messages to Bob will be encrypted using $N = 1717$ and $d = 3$. Bob assumes you cannot factor this N, but you have noticed the prime-factorization $1717 = 17 \cdot 101$. Very well! Use that information to find an integer e that has the feature that

$$\text{for all integers } a, b \qquad \left(b \equiv a^3 \bmod 1717\right) \Rightarrow (a \equiv b^e \bmod 1717)$$

ANSWER: We want to have $a = b^e = (a^3)^e = a^{3e}$. From Euler's Theorem we know that $a^{\phi(N)} \equiv 1 \bmod N$ whenever a is coprime to N, so we will certainly have what we want as long as $3e \equiv 1$ modulo $\phi(N)$. As far as anyone knows, the only way to compute $\phi(N)$ is to first factor N, but in this case we can do that easily. (Bob should have chosen a number N that was harder to factor!) Since $N = 17 \cdot 101$ we get $\phi(N) = 16 \cdot 100 = 1600$. And now it is easy to solve $3e \equiv 1 \bmod \phi(N)$: divide 1600 by 3 to see $1600 = 3 \cdot 533 + 1$, so $3 \cdot 533 \equiv -1 \bmod 1600$, and thus the inverse of 3 is $-533 = 1067$.

Other values of e also work. For example you could use the Chinese Remainder Theorem to note that it is necessary and sufficient to have $a \equiv a^{3e}$ modulo 17 and modulo 101. By the Fermat Theorem the former is true for all a as long as $3e \equiv 1 \bmod 16$, and the latter is true for all a if $3e \equiv 1 \bmod 100$. Thus it suffices to have $3e - 1$ be divisible by lcm(16,100)=400. So we need only solve $3e \equiv 1 \bmod 400$, which requires $e = 3^{-1} \equiv -133 \equiv 267$ modulo 400. (This includes the previous result $e = 1067$.)

For example, Alice would encrypt a 2 as $2^3 = 8$; you (Eve) can now decrypt this: seeing an 8 you would know the original plaintext would have been 8^{267} which can be computed modulo N with eight squarings:

$$8^2 \equiv 64, \quad 8^4 \equiv 64^2 \equiv 662, \quad \ldots, \quad 8^{256} \equiv 239$$

and then three more multiplications:

$$8^{267} = 8^1 \cdot 8^2 \cdot 8^8 \cdot 8^{256} \equiv 2$$