Homework Assignment #2 (100 points, weight 5%)
Due: Thursday, March 15, at 1:00pm (in lecture)

Number Theory and Proof Methods

1. (20 points) We call a positive integer **perfect** if it equals the sum of its positive divisors other than itself.

   (a) Prove that 6 and 28 are perfect numbers.

   We have that $6 = 2 \cdot 3$, so the positive divisors of 6 other than itself are 1, 2, and 3. As $1 + 2 + 3 = 6$, 6 is perfect.

   We have that $28 = 2 \cdot 2 \cdot 7$, so the positive divisors of 28 are 1, 2, 4, 7, and 14. $1 + 2 + 4 + 7 + 14 = 28$, so 28 is perfect.

   (b) Prove that if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is a perfect number.

   The positive divisors of $2^{p-1}(2^p - 1)$ other than itself for $2^p - 1$ prime are all the numbers of the form 2^i for $0 \leq i \leq p-1$, and $2^j(2^p-1)$ for $0 \leq j < p-1$. Note that $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for any positive integer n: this can be seen by thinking of the sum as the binary number $\underbrace{11\ldots1}_{n}$, which is just the binary expression $1\underbrace{0\ldots0}_{n}-1$.

   Thus, taking the sum of these positive divisors gives:

$$\begin{aligned}
\sum_{i=0}^{p-1} 2^i + \sum_{j=0}^{p-2} 2^j(2^p - 1) &= (2^p - 1) + (2^p - 1)(2^{p-1} - 1) \\
&= (2^p - 1)(1 + (2^{p-1} - 1)) \\
&= (2^p - 1)2^{p-1}
\end{aligned}$$

   Thus, for $2^p - 1$ prime, we have that $2^{p-1}(2^p - 1)$ is perfect.

2. (20 points)

   (a) Find the inverse of 19 modulo 141, using the Extended Euclidean Algorithm. Show your steps.

   We apply the Euclidean Algorithm to 19 and 141:

$$\begin{aligned}
141 &= 7 \cdot 19 + 8 \\
19 &= 2 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1
\end{aligned}$$

Thus, $\gcd(19, 141) = 1$, which is a requirement for the inverse to exist. Now we proceed with the rest of the Extended Euclidean algorithm to express $\gcd(19, 141) = 19s + 141t$ for integers s, t. Then we have that s is the inverse of 19 modulo 141:

$$\begin{aligned}1 &= 3 - 1 \cdot 2 \\ &= 3 - (8 - 2 \cdot 3) \\ &= -8 + 3 \cdot 3 \\ &= -8 + 3(19 - 2 \cdot 8) \\ &= 3 \cdot 19 - 7 \cdot 8 \\ &= 3 \cdot 19 - 7(141 - 7 \cdot 19) \\ &= -7 \cdot 141 + 52 \cdot 19\end{aligned}$$

Thus, the inverse of 19 modulo 141 is 52.

(b) Solve the congruence $19x \equiv 7 \pmod{141}$, by specifying all the integer solutions x that satisfy the congruence.

We have that the inverse of 19 modulo 141 is 52, so we can multiply both sides of the equation by 52:

$$\begin{aligned}19x &\equiv 7 \pmod{141} \\ 52 \cdot 19x &\equiv 52 \cdot 7 \pmod{141} \\ x &\equiv 82 \pmod{141}\end{aligned}$$

Thus, the integer solutions that satisfy the congruence are of the form $82 + 141i$ for all integers i.

3. (20 points) Find all solutions of the congruence $x^2 \equiv 16 \pmod{105}$.
Hint: find all the solutions of this congruence modulo 3, modulo 5 and modulo 7 and then use the Chinese Remainder Theorem. Note that each of these equations will have two solutions so when combining them you can expect 8 different solutions mod 105.

We find all of the solutions $x^2 \equiv 16 \equiv 1 \pmod{3}$. There are only two nonzero values modulo 3, namely 1 and 2, and both of these are solutions to the equation.

We then find all solutions $x^2 \equiv 16 \equiv 1 \pmod{5}$. There are two such solutions, namely 1 and 4.

Finally, we find all solutions $x^2 \equiv 16 \equiv 2 \pmod{7}$. There are two such solutions, namely 3 and 4.

For each combination of solutions, we apply the Chinese remainder theorem. We have that $M_1 = 105/3 = 35$, and an inverse of 35 modulo 3 is 2; $M_2 = 105/5 = 21$, and an inverse of 21 modulo 5 is 1; and $M_3 = 105/7 = 15$, and an inverse of 15 modulo 7 is 1. Then, for every combination a_1, a_2, a_3 of solutions with $a_1 = 1, 2$, $a_2 = 1, 4$, and $a_3 = 3, 4$, we have that the following is a solution to the congruence:

$$x \equiv a_1 \cdot 35 \cdot 2 + a_2 \cdot 21 \cdot 1 + a_3 \cdot 15 \cdot 1 = 70a_1 + 21a_2 + 15a_3.$$

For $a_1 = 1$, $a_2 = 1$, $a_3 = 3$, this gives $x \equiv 31 \pmod{105}$, so $x = 31 + 105y$ for all integers y.

For $a_1 = 1$, $a_2 = 1$, $a_3 = 4$, this gives $x \equiv 46 \pmod{105}$, so $x = 46 + 105y$ for all integers y.

For $a_1 = 1$, $a_2 = 4$, $a_3 = 3$, this gives $x \equiv 94 \pmod{105}$, so $x = 94 + 105y$ for all integers y.

For $a_1 = 1$, $a_2 = 4$, $a_3 = 4$, this gives $x \equiv 4 \pmod{105}$, so $x = 4 + 105y$ for all integers y.

For $a_1 = 2$, $a_2 = 1$, $a_3 = 3$, this gives $x \equiv 101 \pmod{105}$, so $x = 101 + 105y$ for all integers y.

For $a_1 = 2$, $a_2 = 1$, $a_3 = 4$, this gives $x \equiv 11 \pmod{105}$, so $x = 11 + 105y$ for all integers y.

For $a_1 = 2$, $a_2 = 4$, $a_3 = 3$, this gives $x \equiv 59 \pmod{105}$, so $x = 59 + 105y$ for all integers y.

For $a_1 = 2$, $a_2 = 4$, $a_3 = 4$, this gives $x \equiv 74 \pmod{105}$, so $x = 74 + 105y$ for all integers y.

Thus, these are all of the solutions to the congruence.

4. (20 points)

   (a) Use Fermat's little theorem to compute: 4^{101} *mod* 5, 4^{101} *mod* 7, 4^{101} *mod* 11.

   First we compute $4^{101} \pmod{5}$. We have that $a^4 \equiv 1 \pmod{5}$ by Fermat's little theorem, so:

$$4^{101} \equiv 4^{4 \cdot 25+1} \equiv 4 \cdot (4^4)^{25} \equiv 4 \cdot 1^{25} \equiv 4 \pmod{5}.$$

   We now compute $4^{101} \pmod{7}$. We have that $a^6 \equiv 1 \pmod{7}$ by Femat's Little Theorem, which gives:

$$4^{101} \equiv 4^{16 \cdot 6+5} \equiv 4^5(4^6)^{16} \equiv 4^5 1^{16} \equiv 4^5 \pmod{7}.$$

   We have that $4^2 \equiv 16 \equiv 2 \pmod{7}$, so this gives that':

$$4^5 \equiv (4^2)^2 4 \equiv (2^2)4 \equiv 4^2 \equiv 2 \pmod{7}.$$

   Finally, we find $4^{101} \pmod{11}$. We have that $4^{10} \equiv 1 \pmod{11}$ by Fermat's Little Theorem, which gives:

$$4^{101} \equiv 4^{10 \cdot 10+1} \equiv 4 \cdot (4^{10})^{10} \equiv 4 \pmod{11}.$$

(b) Use your results from part (a) and the Chinese Remainder Theorem to compute 4^{101} *mod* 385. (note that $385 = 5 \times 7 \times 11$).

We have that $M_1 = 385/5 = 77$, and the inverse of 77 modulo 5 is $y_1 = 3$. As well, $M_2 = 385/7 = 55$, and the inverse of 55 modulo 7 is $y_2 = 6$. Finally, $M_3 = 385/11 = 35$, and the inverse of 35 modulo 11 is $y_3 = 6$. Thus, by the Chinese Remainder Theorem, the solution has the form:

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 4 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 4 \cdot 35 \cdot 6 \equiv 114 \pmod{385}.$$

Thus, $4^{101} \equiv 114 \pmod{385}$.

5. (20 points)
Encrypt the message ATTACK using the RSA cryptosystem with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in example 11 in the textbook and in the classnotes.

We have $p = 43$, $q = 59$, and $n = 2537$. Mapping letters to their positions in the alphabet gives that A has value 1, C has value 3, K has value 11, and T has value 20. Thus, the messages we want to transmit are AT, which has value 0120; TA, which has value 2001; and CK, which has value 0311.

To encrypt message M, we calculate $C = M^e \pmod{n}$. Thus, 0120 encrypts to:

$$C_1 = (0120)^{13} \equiv 286 \pmod{2537}.$$

Then 2001 encrypts to:

$$C_2 = (2001)^{13} \equiv 798 \pmod{2537}.$$

And finally, 0311 encrypts to:

$$C_3 = (0311)^{13} \equiv 425 \pmod{2537}.$$

Thus, the encrypted message is 286, 798, 425.