HOMEWORK 5: DUE APRIL 15

In our discussion in class of the idea of Public Key Encryption we have seen that the well-known RSA method is based on group theory associated with modular arithmetic. The current homework assignment pursues this both further and in detail.

First Basic Result. Let $n$ be a positive integer, not necessarily prime, and set

$$G = \{ r : 1 \leq r < n, \gcd(r, n) = 1 \}.$$  

Then $G$ is a group under multiplication mod $n$.

Problem 1. To illustrate what $G$ can look like, write down all elements $x$ in $G$ when $n = 21$ and then determine the inverse $x^{-1}$ for each of these elements $x$.

To prove the First Basic Result we have to show:

1. $G$ is closed under multiplication mod $n$;
2. $G$ contains an identity element $e$; 
3. for each $x$ in $G$ there exists an inverse $y$ in $G$, i.e., $xy \equiv 1 \pmod{n}$.

Property (2) is clear since $e = 1$ is an identity for $\mathbb{Z}$, hence for multiplication mod $n$. Let’s try proving (1), which is the result we looked at with some difficulty in class. A restatement of (1) is contained in the next problem.

Problem 2. Suppose $r$, $v$ and integers such that

$$1 \leq r, v < n, \quad \gcd(r, n) = 1 = \gcd(v, n),$$

and define $k$ by $rv \equiv k \pmod{n}$. Then $\gcd(k, n) = 1$.

To answer problem 2, complete the following steps:

1. write $rv = k + mn$ for some integer $m$;
2. let $a$ be an integer dividing both $k$ and $n$. Show that we can assume $a$ is prime;
3. show that $a$ divides both $rv$ and $n$;
4. show that $a$ divides either $r$ or $v$ (or both);
5. deduce that $a = 1$, and hence that $\gcd(k, n) = 1$.

Establishing the existence of an inverse for each element in $G$ amounts to solving the next problem.

Typeset by AMS-\TeX
**Problem 3.** Let \( r \) be an integer such that \( 1 \leq r < n \) and \( \gcd (r, n) = 1 \). Then there exists an integer \( s \) such that

\[
1 \leq s < n, \quad rs \equiv 1 \pmod{n}.
\]

To handle Problem 3 we can use Propositions 1.6.2 and 1.6.9 in the text. Fix integers \( r, n \) but let’s not assume for the moment that \( \gcd (r, n) = 1 \). Now define \( I(r, n) \) by

\[
I(r, n) = \{ ar + bn : \ a, b \in \mathbb{Z} \}.
\]

Show that \( I(r, n) \) has the following properties:

1. if an integer \( c \) is a divisor of both \( r \) and \( n \), then \( c \) divides every element of \( I(r, n) \);
2. if \( d = \gcd(r, n) \), then \( d \) belongs to \( I(r, n) \);

Deduce from these properties of \( I(r, n) \) that if \( \gcd (r, n) = 1 \), then there is an integer \( t \) such that \( rt \equiv 1 \pmod{n} \).

**Problem 4.** Show that if there exists an integer \( t \) such that \( rt \equiv 1 \pmod{n} \), then there exists an integer \( s \) such that

\[
1 \leq s < n, \quad rs \equiv 1 \pmod{n}.
\]

This completes the proof of The First Basic Result. As a further illustration of this result, answer

**Problem 5.** Write down all elements \( x \) in \( G \) when \( n = 12 \) and then determine the inverse \( x^{-1} \) for each of these elements \( x \).

**Second Basic Result.** Let \( n \) be an integer, not necessarily prime, and define the so-called Euler \( \phi \)-function by

\[
\phi(n) = \# \{ r : 1 \leq r < n, \ \gcd(r, n) = 1 \}.
\]

Then each integer \( a \) for which \( \gcd(a, n) = 1 \) has the property

\[
a^{\phi(n)} \equiv 1 \pmod{n}.
\]
Problem 6. Use Lagrange’s Theorem and the First Basic Result to give a proof of the Second Basic Result.

Already we have assembled all the results need to describe the RSA Public Key Encryption system: choose a pair of positive, prime integers $p, q$ which in practice will be very large. Now set $n = pq$. At the current state of ‘unclassified’ knowledge, it is very hard to determine the prime factors $p, q$ if one knows only the value of $n$. Next set $m = (p - 1)(q - 1)$.

Problem 7. Show that $\phi(n) = m = (p - 1)(q - 1)$. (This is the significance of making the particular choice of $m$.)

Next fix an integer $e$ such that

$$1 \leq e < m, \quad \text{gcd}(e, m) = 1.$$

Problem 8. Use the First Basic Result to show that there exists an integer $s$ such that

$$1 \leq s < m, \quad es \equiv 1 \pmod{m}.$$

Again at the current state of ‘unclassified’ knowledge, it is very hard to determine $s$ if one knows only $n$ and $e$. So one can feel reasonably secure telling everyone the values of $n$ and $e$. The RSA system proceeds as follows: suppose $a$ is an integer such that

$$1 \leq a < n, \quad \text{gcd}(a, n) = 1;$$

when $n$ is large, there will be very few choices $a$ for which $\text{gcd}(a, n) > 1$ (can you see why?). Set $b = a^e \pmod{n}$.

Problem 9. Use the First and Second Basic Results to show that $a = b^s \pmod{n}$. In other words, we can recover the value $a$ from $b$ provided we know $s$.

Problem 10. Use your answers to problems 1 and 5 to illustrate the RSA Public Key Encryption system when $p = 7$ and $q = 3$. 