2nd Cryptography Homework

3.13.4.a Use the Euclidean algorithm to compute $gcd(30030, 257)$.

$$30030 = 257 \cdot 116 + 218$$

$$257 = 218 \cdot 1 + 39$$

$$218 = 39 \cdot 5 + 23$$

$$39 = 23 \cdot 1 + 16$$

$$23 = 16 \cdot 1 + 7$$

$$16 = 7 \cdot 1 + 2$$

$$7 = 2 \cdot 3 + 1$$

Hence $\gcd(30030, 257) = 1$.

3.13.4.b Using the result of part (a) and fact that $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, show that 257 is prime.

Since $\gcd(30030, 257) = 1$ and $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, We obtain that $\gcd(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 257) = 1$ and the next prime $17^2 = 289 > 257$. 257 is a prime.

3.13.10 A group of people are arranging themselves for a parade. if they line up three to a row, one person is left over, if they line up four to a row, two people are left over and if they line up five to a row, three people one left over. What is the smallest possible number of people? What is the next smallest number? (HINT: interpret in CRT).

Assume there is x people and we know that

$$x = 1 \pmod 3$$

$$x = 2 \pmod 4$$

$$x = 3 \pmod 5$$

$$n = 3 \cdot 4 \cdot 5 = 60$$

$$m_1 = 1, m_2 = 2, m_3 = 3$$

$$r_1 = 3, r_2 = 4, r_3 = 5$$

$$z_1 = 20, z_2 = 15, z_3 = 12$$

and $x = 20 \cdot 2 \cdot 1 + 15 \cdot 3 \cdot 2 + 12 \cdot 3 \cdot 3 = 58 \pmod{60}$. The smallest number of people is 58 and the next is 118.

3.13.13 Find the last 2-digits of 123^{562}

$100 = 2^2 \cdot 5^2$ and $\phi(100) = 100(1-\frac{1}{2})(1-\frac{1}{5}) = 10$. By using Euler's Theorem, we obtain that

$$123^{562} = 123^{562 \pmod{10}} = 123^2 = 29 \pmod{100}.$$

The last 2 digits is 29.

3.13.17.a Show that every nonzero congruence class mod 11 is a power of 2, and therefore 2 is a primitive root mod 11.

Since $\phi(11) = 10 = 2 \cdot 5$, $2^2 = 4 \pmod{11}$, and $2^5 = 10 \pmod{11}$, we know that 2 is a primitive root mod 11.

3.13.17.b Note that $2^3 = 8 \pmod{11}$. Find x such that $8^x = 2 \pmod{11}$ (Hint: What is inverse of $3 \pmod{10}$?)

Since $2^3 = 8 \pmod{11}$, and $3 \cdot 7 = 1 \pmod{10}$. $8^7 = 2^{3\cdot 7 \pmod{10}} = 2 \pmod{11}$, and $x = 7$.

3.13.17.c Show that every nonzero congruence class mod 11 is a power of 8, and therefore 8 is a primitive root mod 11

Since $\phi(11) = 10 = 2 \cdot 5$, $8^2 = 9 \pmod{11}$, and $8^5 = 10 \pmod{11}$, we know that 8 is a primitive root mod 11.

3.13.17.d Let p be prime and let g is a primitive root mod p. Let $h = g^y \pmod{p}$ with $\gcd(y, p-1) = 1$. Let $xy = 1 \pmod{p-1}$. Show that $h^x = g \pmod{p}$.

Since $\gcd(y, p-1) = 1$ and Fermet's little theorem, $h^x = g^{yx \pmod{p-1}} = g \pmod{p}$.

3.13.17.e Let p and h as in part (d) Show that h is a primitive root $\mod p$.(Remark: Since there are $\phi(p-1)$ possibilities for the exponent x in part (d), this yields all of the $\phi(p-1)$ primitive root mod p)

By 3.13.17.d, we know that $h^x = g \pmod{p}$ and g is a primitive $\pmod{p}$. For any element i in Z_p^*, there exists j s.t. $i = g^j \pmod{p}$ and $i = (h^x)^j \pmod{p}$. Hence h is a primitive $\pmod{p}$.

3.13.20 Let a and $n > 1$ be integers with $\gcd(a, n) = 1$. The order of $a \mod n$ is the smallest positive integer r such that $a^r = 1 \pmod{n}$. We denote $r =_{ord_n} (a)$

3.13.20.a Show that $r \le \phi(n)$

Since $a^r = 1 \pmod{n}$, $a^{\phi(n)} = 1 \pmod{n}$ and r is the smallest positive integer, we obtain that $r \le \phi(n)$.

3.13.20.b Show that if $m = rk$ is a multiple of r, then $a^m = 1 \pmod{n}$.

Since $a^r = 1 \pmod{n}$, $a^m = a^{rk} = (a^r)^k = 1^k = 1 \pmod{n}$.

3.13.20.c Suppose $a^t = 1 \pmod{n}$. Write $t = qr + s$ with $0 \le s < r$. Show that $a^s = 1 \pmod{n}$.

Since $a^t = a^{qr+s} = a^{qr} \cdot a^s = 1 \cdot a^s = 1 \pmod{n}$, then $a^s = 1 \pmod{n}$.

3.13.20.d Using definition of r and fact that $0 \le s < r$, show $s = 0$, and therefore $r|t$. This, combined with part (b), yields the result that $a^t = 1 \pmod{n}$ iff $ord_n(a)|t$.

Since $a^s = 1 \pmod{n}$, $0 \le s < r$ and r is the smallest number s.t. $a^r = 1 \pmod{n}$, $s = 0$ and $t = qr + 0 = qr$, we conclude that $r|t$. Then we know that $r = ord_n(a)|t$. And 3.13.20.b declares that if $r|t$, then $a^t = 1 \pmod{n}$.

3.13.20.e Show that $ord_n(a)|\phi(n)$.

Assume $\phi(n) = qr + s$. Since $a^{\phi(n)} = 1 \pmod n$ and 3.13.20.d, we will obtain that $s = 0$ and $ord_n(a)|\phi(n)$.

3.13.30.a Let n be odd and assume $\gcd(a, n) = 1$. Show that if $(\frac{a}{n}) = -1$, then a is not a square mod n.

Since $(\frac{a}{n}) = -1$, a is not square for some mod p_i that divides n, then a is not a square mod n.

3.13.30.b Show that $(\frac{3}{35}) = +1$

$(\frac{3}{35}) = (\frac{3}{5})(\frac{3}{7}) = (-1)(-1) = +1.$

3.13.30.c Show that 3 is not square mod 35.

Since $(\frac{3}{5}) = (\frac{3}{7}) = -1$, 3 is not a square $\pmod 5$ and $\pmod 7$. 3 cannot be a square $\pmod{35}$.

3.13.39 Let p and q be distinct primes.

3.13.39.a show that among the integers m satisfying $1 \le m < pq$, there are $q - 1$ multiplies of p, and there are $p - 1$ multiplies of q

the $q-1$ multiplies of p are p,$2p$,$3p$,$\cdots$,$(q-1)p$ and the $p-1$ multiplies of q are q,$2q$,$\cdots$,$(p-1)q$.

3.13.39.b Suppose $\gcd(m, pq) > 1$. Show that m is a multiple of p or a multiple of q.

Assume $\gcd(m, pq) = d > 1$, $d|m$ and $d|pq$. Since p and q are primes, d must be $1, p, q$ or pq to satisfy $d|pq$. Note that $d > 1$, we obtain that $p|m$ or $q|m$.

3.13.39.c Show that if $1 \le m < pq$, then m cannot be a multiple of both p and q.

Since p, q are distinct primes if m can be a multiple of both p and q. It means that $m = kpq \ge pq$.(Contradiction)

3.13.39.d Show that the number of integers m with $1 \le m < pq$ such that $\gcd(m, pq) = 1$ is $pq-1-(p-1)-(q-1) = (p-1)(q-1)$ (Remark:$\phi(pq) = (p-1)(q-1)$)

The number of integers m with $1 \le m < pq$ is $pq - 1$, and there are $q - 1$ multiplies of p and $p - 1$ multiplies of q. We obtain that the number of integers m with $1 \le m < pq$ s.t. $\gcd(m, pq) = 1$ is $pq - 1 - (p - 1) - (q - 1) = pq - 1 - p + 1 - q + 1 = pq - p - q + 1 = (p - 1)(q - 1)$.

3.14.10 Let

$$M = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 5 & 25 \\ 1 & 14 & 196 \end{pmatrix}.$$

3.14.10.a Find the inverse of $M \pmod{101}$.

$$M^{-1} = \begin{pmatrix} 30 & 85 & 88 \\ 64 & 38 & 100 \\ 87 & 86 & 29 \end{pmatrix} \pmod{101}.$$

3.14.10.b For which primes p does M not have an inverse mod p?

The primes p s.t. $\gcd(p, 324) \ne 1$. (Det(M)=324.)