**Elementary Number Theory**
**27th October 2021**

Here is an interesting application of CRT:

**Lemma.** *Let $n$ be any positive integer and let $a, b, c, d \in \mathbb{Z}$ satisfy $ad-bc \equiv 1$ mod $n$. Then, one may change $a, b, c, d$ mod $n$ such that the new $a, b, c, d$ satisfy $ad - bc = 1$.*

**Proof.**

We use the Chines remainder theorem. Let $a, b, c, d \in \mathbb{Z}$ such that $ad-bc \equiv 1$ mod $n$. Write $ad - bc = 1 + qn$. Note that $(c, d, n) = 1$. We would like to change $a, b, c, d$ mod $n$ so that $ad - bc$ becomes 1.

First, let us suppose that $(c, d) = 1$. Consider $a' = a + un$ and $b' = b + vn$ where $u, v$ are to be chosen such that $a'd - b'c = 1$.

Now $a'd - b'c = ad - bc + (ud - vc)n = 1 + (q + ud - vc)n$.

Since $(c, d) = 1$, we may choose $u, v$ with $q = vc - ud$; this gives $a'd - b'c = 1$ and we have done.

So, we only have to prove that the above supposition $(c, d) = 1$ can be assumed by changing $c, d$ modulo $n$. Let $p_1, \cdots, p_r$ be the set of all primes which divide $d$. If each $p_i | n$, then clearly, none of the $p_i$'s divide $c$ since $(c, d, n) = 1$. In such a case, evidently, $(c, d) = 1$.

So, let us suppose that some of the $p_i$'s do not divide $n$; let $p_1, \cdots, p_k$ be the subset of these primes. We note that $(n, p_1, \cdots p_k) = 1$. By the Chinese remainder theorem, choose an integer $x \equiv c$ mod $n$ and $x \equiv 1$ mod $p_1 \cdots p_k$. Then, clearly $p_1, \cdots, p_k \not| x$.

Also, writing $x = c + ln$, we have that the other $p_i$'s which divide $n$ cannot divide $c + ln$ as $(c, d, n) = 1$. Hence $(c + ln, d) = 1$ and we are done.

**Q 14, P. 127, Tom Apostol's book.** Given positive integers $a, b, x_0$ and the sequence defined recursively by $x_{n+1} = ax_n + b$, we need to show that not all $x_i$'s can be prime.

First, suppose $a = 1$. Then, clearly $x_{x_1+1} = x_1 + x_1 b$ cannot be prime as $x_1 > 1$ being a prime.

Now, if $a \neq 1$, there exists some $i$ so that $a - 1 \not\equiv 0$ mod $x_i$. Fix such an $i$. Let the order of $a$ mod $x_i$ be $n$; then $a^n \equiv 1$ but $a \not\equiv 1$ mod $x_i$. By induction, we see that

$$x_{n+i} = a^n x_i + (a^{n-1} + a^{n-2} + \cdots + a + 1)b.$$

But, $x_i$ is prime and divides $a^n - 1 = (a - 1)(a^{n-1} + \cdots + a + 1)$ while it does not divide $a - 1$. Therefore, the above RHS is a proper multiple of $x_i$ and thus $x_{n+i}$ cannot be prime.

**Q 41, P.74, NZM.** If $f(n)$ is the sum of positive integers less than and prime to $n$, we need to show $f$ is 1-1.

We can see $f(n) = n\phi(n)/2$ for $n > 1$ (this is problem 40 and is easy to see

because $r$ is co-prime to $n$ if and only if $n-r$ is).
To prove 1-1-ness, suppose $n\phi(n) = m\phi(m)$. Let $p$ be the largest prime dividing either side, say $p^k||n$. Note that the precise power $v_p$ of $p$ dividing $n\phi(n)$ is $2k-1$ as $p$ is the largest prime dividing $n$. Clearly, by this argument, the power of $p$ dividing $m\phi(m)$ must also be $2k-1$. Then, writing $n = p^kN, m = p^kM$, we have $n\phi(n) = p^{2k-1}N\phi(N) = p^{2k-1}M\phi(M)$. Therefore, $N\phi(N) = M\phi(M)$. We may proceed inductively to deduce $m = n$.

**Q 42.** We need to find all $n$ for which $n/\phi(n)$ is an integer. Clearly, $n = 2^r$ are solutions (for $r \geq 0$). Now, let $n > 1$ be any solution with at least one odd prime divisor. Write $n = \prod_p p^{v_p}$ as a product of prime powers. Then, $\phi(n) = n\prod_p(1-1/p)$. So, writing $n = \prod_{i=1}^r p_i^{v_i}$, we have

$$\prod_{i=1}^{r} \frac{p_i}{p_i - 1} \in \mathbb{N}.$$

We write $p_1 < p_2 < \cdots < p_r$ for convenience. Then, $p_1 - 1$ is coprime to the numerator $\prod_i p_i$ which means $p_1 = 2$. Also, the power of 2 dividing the denominator $\prod_{i=1}^r (p_i - 1)$ is at least by $r-1$ and this must divide $p_1 = 2$ which means $r = 2$. Thus, $\frac{n}{\phi(n)} = \frac{2p_2}{p_2-1}$ which can be an integer if and only if $p_2 - 1$ divides $2p_2$ and hence divides 2 so that we must have $p_2 = 3$. Hence. $n = 2^u3^v$ are all the solutions.

**Q 43.** We need to show $n - \phi(n) < d - \phi(d)$ for each divisor $d$ of $n$ with $d < n$.
Indeed, $n-\phi(n)$ is the set of all $a \leq n$ which are NOT coprime to $n$. Clearly, the number $d-\phi(d)$ of integers $b \leq d$ which are NOT coprime to $d$ are among the $a$'s and hence we have$n - \phi(n) \geq d - \phi(d)$. Strict inequality follows by including the number $n$.
• We prove that any $n > 1$ has a prime factor smaller than every prime factor of $3^n - 2^n$.
Let $p$ be the smallest prime factor of $3^n - 2^n$. So, $(p, 6) = 1$. So, $2a \equiv 1 \mod p$. Hence $(3a)^n \equiv (2a)^n \equiv 1 \mod p$.
Thus, the order $d$ of $3a \mod p$ divides $d|(n, p-1)$.
Of course $d \neq 1$ (otherwise, $3a \equiv 1 \equiv 2a \mod p$, a contradiction).
So, the smallest prime divisor of $n$ is $\leq$ any prime divisor of $d$ and, therefore, of $p-1$; so, it is $< p$.

**Exercise.** Prove that $n$ does not divide $2^n - 1$ for any $n > 1$.

**Problem 12, P.97.** For any prime $p \geq 5$, we need to prove $\binom{mp-1}{p-1} \equiv 1 \mod p^3$ for any $m \geq 1$.
Then, modulo $p^3$, we have

$$\binom{mp-1}{p-1} - 1 = \frac{(mp-1)(mp-2)\cdots(mp-p+1) - (p-1)(p-2)\cdots 1}{(p-1)!}$$

$$\equiv \frac{1}{(p-1)!}((-mp+p)(\sum_{i=1}^{p-1}\frac{1}{i})(p-1)!+(m^2-1)p^2(\sum_{i<j\leq p-1}\frac{1}{ij})(p-1)!\equiv 0$$

because $\sum_i \frac{1}{i} \equiv 0 \bmod p^2$ by Wolstelholme and $2\sum_{i<j}\frac{1}{ij} \equiv 0 \bmod p$ as we saw earlier.

**Problem 13.**
Note that $\binom{rp}{p} \equiv r \bmod p^3$ by the above problem for $p \geq 5$. So

$$\frac{(mp)!}{(p!)^m} = \binom{mp}{p}\binom{(m-1)p}{p}\cdots\binom{2p}{p} \equiv m!\ mod\ p^3.$$

This proves $(mp)! \equiv (m!)(p!)^m \bmod p^{m+3}$.

**Generalization of Problem 14.**
*For any integer $n \geq 1$ and odd prime $p$, we have the following congruences mod $p$ :*

$$\frac{n^p-n}{p} \equiv -\sum_{r=1}^{p-1}\frac{1^r+2^r+\cdots+n^r}{r} \cdots\cdots (A)$$

*For $n \geq 2$,*

$$\frac{n^p-n}{p} \equiv -\sum_{r=1}^{p-1}\frac{(-1)^r(1^r+2^r+\cdots+(n-1)^r)}{r} \cdots\cdots (A')$$

*In particular, we have the congruences*

$$\frac{2^p-2}{p} \equiv -\sum_{j=1}^{p-1}\frac{2^j}{j} \cdots\cdots\cdots (B)$$

$$\frac{2^p-2}{p} \equiv -\sum_{j=1}^{p-1}\frac{(-1)^j}{j} \cdots\cdots\cdots (C)$$

.
Let us see how. Writing

$$\frac{a^p-a}{p} = \frac{(a+1-1)^p-a}{p} = \sum_{r=1}^{p-1}\binom{p}{r}\frac{(a+1)^r(-1)^{p-r}}{p} + \frac{(a+1)^p-(a+1)}{p}$$

we get, on using the congruence $\frac{\binom{p}{r}}{p} \equiv \frac{(-1)^{r-1}}{r} \bmod p$, that

$$\frac{a^p-a}{p} = \sum_{r=1}^{p-1}\frac{(a+1)^r}{r} + \frac{(a+1)^p-(a+1)}{p} \cdots\cdots (\spadesuit)$$

Putting $a = 0$ gives the well-known congruence $\sum_{r=1}^{p-1}\frac{1}{r} \equiv 0$.
Putting $a = 1$ gives congruence (B).

Putting $a = -2$ gives the congruence (C).
Inductively, from (♠), one gets then that

$$\frac{n^p - n}{p} \equiv -\sum_{r=1}^{p-1} \frac{2^r + \cdots + n^r}{r}.$$

When $p$ is an odd prime, $\sum_{r=1}^{p-1} \frac{1}{r} \equiv 0 \bmod p$ (indeed, it is even zero modulo $p^2$ when $p > 3$ by Wolstenholme's theorem !). Thus, we have the more symmetric form asserted as (A). Finally, (A') is gotten similarly to (A) inductively from (♠) by putting $a = -2, -3, -4$ etc.

**Counting proof for a congruence.**
We had observed using Lucas's theorem that for a prime $p$, $\binom{pn}{pr} \equiv \binom{n}{r} \bmod p$. We now show by *counting* that this congruence holds modulo $p^3$ when $p > 3$.
Consider a $n \times p$ grid of squares from which we select $pr$ squares. We may choose $r$ entire rows; otherwise, there are at least two rows from which between 1 and $p-1$ squares are chosen. Cyclically shifting the squares in each row divides the choices into equivalence classes out of which $\binom{n}{r}$ classes are singletons. The other classes are all of cardinalities multiples of $p^2$. Thus, we have, first of all,

$$\binom{pn}{pr} \equiv \binom{n}{r} \; mod \; p^2$$

We refine this argument now. If a choice of $pr$ squares has less than $r-2$ entire rows, the corresponding equivalence class has cardinality a multiple of $p^3$. Therefore, the asserted congruence mod $p^3$ reduces to showing the special case $\binom{2p}{p} \equiv 2 \bmod p^3$ when $p \geq 5$.
To see this, note

$$\binom{2p}{p} = \sum \binom{p}{k}^2 \equiv 2 + p^2 \sum_{k=1}^{p-1} k^{-2} \; mod \; p^3$$

The latter sum is clearly $\equiv \sum_{k=1}^{p-1} k^2 \equiv 0 \bmod p$ when $p > 3$.

**Primes congruent to 1 mod $n$**

If $d$ is a positive integer, then for the arithmetic progression $\{nd+1; n \geq 1\}$, one can use cyclotomic polynomials to prove this. In fact, when $d = 2$, this reduces to Euclid's argument!
Before proceeding further, we just point out that there are arbitrarily large gaps in the sequence of primes; for any $n \geq 2$, just observe that the $n$ consecutive numbers $n! + 2, n! + 3, \cdots, n! + n$ are all composite.

The cyclotomic polynomials are defined as follows.
For any $n$, the polynomial $x^n - 1 = \prod_{r=1}^{n}(x - e^{2ir\pi/n})$ has the complex $n$-th roots of unity as its roots. Note that the roots are the powers of $\zeta = e^{2i\pi/n}$. The root $\zeta$ has 'order' $n$; that is, it is the smallest power raised to which gives the value 1 (unity). A root $\zeta^r$ has order $n/(n, r)$ clearly. Thus, $\zeta^r$ has order $n$ if, and only if, $(r, n) = 1$. One defines the cyclotomic polyonomial $\Phi_n$ as

$$\Phi_n(x) = \prod_{(r,n)=1} (x - \zeta^r)$$

where the product is over the integers $\leq n$ which are coprime to $n$. The first interesting property of $\Phi_n(x)$ is that it has integer coefficients. To see this, first note that

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

as $n$-th roots of unity can be partitioned into disjoint sets $S_d$ for $d|n$ consisting of those roots whose orders equal $d$. Let us prove that $\Phi_n(x)$ has integer coefficients, by induction on $n$. If $n = 1$, then $\Phi_1(x) = x - 1$; so, it is ok. Assume $n > 1$ and that $\Phi_d(x)$ has integer coefficients for any $d < n$. Then, the equality

$$x^n - 1 = \Phi_n(x) \prod_{d|n, d<n} \Phi_d(x)$$

shows that $x^n - 1 = \Phi_n(x)f(x)$ where $f$ is a monic polynomial with integer coefficients by induction hypothesis. Then, it is an easy exercise to see inductively that the coefficients of $\Phi_n(x)$ are integers (from the top coefficients downwards).

Suppose $p_l, p_2, \cdots, p_r$ are prime numbers in the arithmetic progression 1 mod $d$. We will use cyclotomic polynomials to produce another prime $p$ in this progression different from the above $p_i$'s. This would imply that there are infinitely many primes in such a progression. We will use the simple observation that a polynomial $p(X)$ with integer coefficients has the property that $p(m) - p(n)$ is an integer multiple of $m - n$.

Consider the number $N = dp_l p_2 \cdots p_r$. Then, for any integer $n$, the two values $\Phi_d(nN)$ and $\Phi_d(0)$ differ by a multiple of $N$. But, $\Phi_d(0)$ is an integer which is also a root of unity and must, therefore, be $\pm 1$. Moreover, as $n \to \infty$, the values $\Phi_d(nN) \to \infty$ as well since $\Phi_d$ is a nonconstant monic polynomial. In other words, for large $n$, the integer $\Phi_d(nN)$ has a prime factor $p$. As $\Phi_d(nN)$ is $\pm 1$ modulo any of the $p_1, p_2, \cdots, p_r$ and modulo $d$, the prime $p$ is different from any of the $p_i$'s and does not divide $d$.
Which primes divide some value $\Phi_d(a)$ of a cyclotomic polynomial?
The answer is that they are precisely the primes $\equiv 1$ mod $d$.
To show this, it is enough to prove that if $p$ is a prime not dividing $d$ but divides $\Phi_d(a)$ for some integer $a$, then $a$ has order $d$ in the group $\mathbb{Z}_p^{|ast}$ (hence, $d$ divides the order $p - 1$).
Let us prove this now. Since $X^d - 1 = \prod_{l|d} \Phi_l(X)$, it follows that $p$ which divides $\Phi_d(a)$ has to divide $a^d - 1$ also. If $d$ were not the order of $a$, let $k$ divide $d$ with $k < d$ and $p$ divides $a^k - 1$. Once again, the relation $a^k - 1 = \prod_{l|k} \Phi_l(a)$ shows that $p$ divides $\Phi_l(a)$ for some positive integer $l$ dividing $k$. Therefore, $p$ divides both $\Phi_d(a + p)$ and $\Phi_l(a + p)$. Now,

$$(a + p)^d - 1 = \prod_{m|d} \Phi_m(a + p) = \Phi_d(a + p)\Phi_l(a + p) \ (other\ terms).$$

The expression on the right hand side is divisible by $p^2$. On the other hand, the left side is equal, modulo $p^2$, to $a^d + dpa^{d-1} - 1$. Since $p^2$ divides $a^d - 1$, it must divide $dpa^{d-1}$ as well. This is clearly impossible since neither $a$ nor $d$ is divisible by $p$. This proves that any prime factor $p$ of $\Phi_d(nN)$ occurs in the arithmetic progression $\{1 + nd; n > 0\}$ and thereby, proves the infinitude of the primes in this progression. Interestingly, Euclid's classical proof of the infinitude of prime numbers is the special case of the above proof where we can use $d = 2$.

**RSA cryptosystem**

This is the most popular of public key cryptosystems in use today. It was a system described by Rivest, Shamir and Adleman in 1977. It is based on the following elementary fact from number theory. If $p \neq q$ are primes and $n = pq$, then the number $\phi(n) = (p-1)(q-1)$ satisfies Euler's congruence $a^{\phi(n)} \equiv 1 \bmod n$ for any $(a, n) = 1$. Let us describe the RSA system now.

**I.** Each user A selects two large primes $p_A \neq q_A$. Write $n_A = p_A q_A$.
**II.** Each user A selects a large random $d_A$ such that $(d_A, \phi(n_A)) = 1$.
**III.** Each user A determines the unique $e_A \leq \phi(n_A)$ such that $e_A d_A \equiv 1 \bmod \phi(n_A)$. Note also that $(e_A, \phi(n_A)) = 1$.
**IV.** Each user A keeps $p_A, q_A, d_A$ private.
**V.** The numbers $n_A, e_A$ are made public.
**VI.** Plaintexts are represented by a sequence of integers between 0 and $n_A - 1$.
**VII.** Public can use the enciphering transformation

$$f_A : \mathbf{Z}/n_A\mathbf{Z} \to \mathbf{Z}/n_A\mathbf{Z} \ ; \ P \mapsto P^{e_A} \ mod \ n_A$$

to send messages to A. The inverse of $f_A$ is $C \mapsto C^{d_A} \bmod n_A$ is known only to A.

**Why it works :**
First, mathematically, A can read the message because of the following reason. If $(P, n_A) = 1$, that is clear from Euler's congruence. If $p_A | P$, then $q_A \not| P$ as $P < p_A q_A$; so

$$P^{e_A d_A} = P^{1+t(p_A-1)(q_A-1)} \equiv P \ mod \ q_A.$$

Evidently

$$P^{e_A d_A} \equiv 0 \equiv P \ mod \ p_A.$$

Now, knowing $p_A.q_A$ (which A does), it is easy to compute their product $n_A$ as well as $\phi(n_A) = (p_A - 1)(q_A - 1)$. Also, raising to a power is not considered time-consuming as it can be done by a method of repeated squaring. However, only knowing $n_A$, it is very difficult, in practical terms, to factorise and obtain $p_A$ and $q_A$. Knowing $\phi(n_A)$ is also equivalent to knowing $p_A$ and $q_A$ because $\phi(n_A) = n_A - p_A - q_A + 1$ would give us $p_A + q_A$.
*It is unknown as yet as to how to break RSA without factoring $n_A$.*

**Signature through RSA**
To send her signature S to Beena, Alka proceeds as follows. Note that the numbers $n_A, n_B$ for Alka and Beena (although public) are usually different. To deal with this, Alka sends $f_B f_A^{-1}(S)$ if $n_A < n_B$ and sends $f_A^{-1} f_B(S)$ if $n_A \geq n_B$. These are, respectively, $(S^{d_A} \bmod n_A)^{e_B} \bmod n_B$ and $(S^{e_B} \bmod n_B)^{d_A} \bmod n_A$.

**Example.**
As mentioned earlier, small primes $p, q$ should be avoided in order that factorisation is computaionally infeasible. However, for the sake of demonstration, let us take small primes. Let A have the public key $(n, e) = (6012707, 3674911)$. Actually, she has chosen the primes $p = 2357$ and $q = 2551$ and has computed $n = pq = 6012707$ and $\phi(n) = 6007800$. Her enciphering key, she takes to be $e = 3674911$ and, therefore, her deciphering key is $d = 422191$. To encipher the message $m = 5234673$ to be sent to A, a sender B (computes and) sends $c = m^e \bmod n$; this equals 3650502. On receiving this, A deciphers $m$ by computing $c^d \bmod n$.