Number Theory Notes
November 21, 2021

Here are some problems on primitive roots - most were solved in class.

Problem 26, Page 107, NZM (Korselt's criterion).
We need to prove that a composite n is a Carmichael number (that is, n divides $a^{n-1} - 1$ for each a co-prime to n) if, and only if, n is square-free and, for each prime divisor p of n, the number $p - 1$ divides $n - 1$.
Now, first let $n = p_1 p_2 \cdots p_r$ be a square-free number such that for each $i \leq r$, the number $p_i - 1$ divides $n - 1$.
Evidently, for every a co-prime to n, a is co-prime to each p_i; thus, one has by Fermat's little theorem that $a^{p_i - 1} \equiv 1 \bmod p_i$.
So, $a^{n-1} = (a^{p_i-1})^* \equiv 1 \bmod p_i$. In other words, p_i divides $a^{n-1} - 1$ for each $i \leq r$.
Thus, $n = p_1 p_2 \cdots p_r$ itself divides $a^{n-1} - 1$. This shows that n is a Carmichael number.
Conversely, let n be a Carmichael number. If p is a prime dividing n, consider a natural number a of 'order' $p - 1 \bmod p$.
We claim that we can always choose such an a which is co-prime to n.
First, if a is co-prime to n, then by hypothesis, $a^{n-1} \equiv 1 \bmod n$, which implies $a^{n-1} \equiv 1 \bmod p$, and thus $p - 1$ divides $n - 1$.
If $(a, n) > 1$, then look at the set of primes $p = p_1, \cdots, p_k$ which divide n but not a and consider $a + p_1 \cdots p_k$ in place of a.
Evidently, $a + p_1 \cdots p_k$ is co-prime to n; moreover, its order mod p is the same as that of a.
Now, let p^2 divide n for some prime p, if possible. Let b be of order $p(p-1)$ mod p^2. If b is co-prime to n, then $b^{n-1} \equiv 1 \bmod n$ which gives $b^{n-1} \equiv 1 \bmod p^2$ which again implies that $p(p-1)$ divides $n - 1$. Thus p divides $(n - 1)$, an impossibility because p divides n. So, n must be square-free if the b can be chosen co-prime to n.
But, if $(b, n) > 1$, then once again we look at the set of primes $p = p_1, p_2, \cdots, p_k$ which divide n but not b. Then $b + p_1^2 p_2 \cdots p_k$ is co-prime to n and has the same order mod p^2 as b has, namely, $p(p-1)$.

Problems 30, 31; Page 107.

Let $(10p, q) = 1$, and u be the order of 10 mod q. We need to show that the decimal expansion of p/q is eventually periodic with minimum period u. Let k be the minimum period of the fraction. Now

$$\frac{p}{q} = a + 0.f_1 \cdots f_r\ \overline{d_1 d_2 \cdots d_k}$$

where a is a non-negative integer and f_i, d_j's are digits between 0 and 9. Hence,

$$(\frac{p}{q} - a)10^r - f = 0.\overline{d_1 \cdots d_k}$$

where f is the integer with the digits $f_1, \cdots, f_r$. But, $R := 0.\overline{d_1 \cdots d_k}$ satisfies $10^k R - d = R$ where d is the number with digits $d_1, \cdots, d_k$. So,

$$R = \frac{d}{10^k - 1}.$$

Hence,

$$(\frac{p}{q} - a)10^r - f = \frac{d}{10^k - 1}.$$

Write this in integers as

$$(10^r(p - aq) - qf)(10^k - 1) = dq.$$

Hence q divides $10^k - 1$ as it is coprime to p and 10. So, $10^k \equiv 1$ mod q. Thus, the order u of 10 mod q satisfies $u|k$.

Write $10^u - 1 = qm$ say. Also, $k = uv$ say. So, $10^k - 1 = \frac{10^k-1}{10^u-1} qm$. Putting this, we get

$$(1 + 10^u + \cdots + 10^{(v-1)u})qm(10^r(p - aq) - qf) = dq.$$

So, $1 + 10^u + \cdots + 10^{(v-1)u}$ divides d. This means d is obtained by putting a u-digit number D repeated v times. As k is the minimal period, this is possible only when $d = D$; that is, $v = 1$. Hence $k = u$.

Condition for twin primes.
Let $n \geq 2$. Then, both n and $n+2$ are primes if, and only if,

$$4((n-1)!+1)+n \equiv 0 \;\; mod \;\; (n(n+2)).$$

Assume first that the congruence holds. Then $n \neq 2, 4$. So, we have

$$(n-1)!+1 \equiv 0 \;\; mod \;\; n.$$

So, n is prime. Also,

$$4(n-1)!+2 \equiv 0 \;\; mod \;\; n+2.$$

Multiplying by $n(n+1)$, we have

$$4((n+1)!+1)+2(n-1)(n+2) \equiv 0 \;\; mod \;\; n+2.$$

Thus, again it follows by Wilson that $n+2$ must be prime.
Conversely, suppose $n, n+2$ be primes.

$$(n-1)!+1 \equiv 0 \;\; mod \;\; n;$$

$$(n+1)!+1 \equiv 0 \;\; mod \;\; n+2.$$

As $n(n+1) = (n+2)(n-1)+2$, we get $2(n-1)!+1 = d(n+2)$ for some d.
Thus, $2k+1 \equiv 0 \bmod n$ as $(n-1)! \equiv -1 \bmod n$.
Now $4(n-1)!+2 \equiv 0 \equiv -(n+2) \bmod n+2$.
Moreover, $4(n-1)!+2 \equiv 4k \equiv -2 \equiv -(n+2) \bmod n$.
Hence,

$$4(n-1)!+2 \equiv -(n+2) \;\; mod \;\; n(n+2);$$

that is,

$$4((n-1)!+1)+n \equiv 0 \;\; mod \;\; n(n+2).$$

Condition for primality.
Let p be prime not congruent to 1 mod 3. Assume that $4^p \equiv 1$ mod $2p+1$. Then, $2p+1$ is prime.
Let q be any prime factor of $2p+1$. Hence q is odd.
We claim that $q \equiv 1 \bmod p$.
As $4^p \equiv 1 \bmod 2p+1$, we have $4^p \equiv 1 \bmod q$. The order of 4 mod q is 1 or p. If the order is 1, then $q = 3$ and so, $2p+1 \equiv 0 \bmod 3$ which means $p \equiv 1 \bmod 3$, a contradiction.

Hence $p|(q-1)$. So, $q \geq p+1 > \sqrt{2p+1}$. Thus means each prime factor of $2p+1$ is $> \sqrt{2p+1}$. Hence, $2p+1$ must be itself prime.

.

Here are some exercises from IR (Ireland-Rosen's text). The acronym QRL refers to the quadratic reciprocity law which will be discussed later. The problems below have been solved avoiding its use.

Exercise 1, Page 48, Chapter 4, I-R.
Let us show 2 is not a primitive root modulo 29. Indeed, the order of 2 has to divide 28 and is, thus, among $1, 2, 4, 7, 14, 28$. Clearly, $2^4 = 16, 2^7 = 128 \equiv 12, 2^{14} \equiv 14^2 = 144 \equiv -1$ mod 29. Hence, the order must be 28.

Exercises 4,5;, Page 48, Chapter 4, I-R.
Let p be an odd prime.
If $p \equiv 1$ mod 4, we will show that $< a >= \mathbb{Z}_p^*$ if, and only if, $< -a >= \mathbb{Z}_p^*$.
If $p \equiv 3$ mod 4, we will show that $< a >= \mathbb{Z}_p^*$ if, and only if, $-a$ has order $(p-1)/2$ in $\mathbb{Z}_p^*$.
Let $p \equiv 1$ mod 4 first.
If a is a primitive root mod p, then clearly $a^{(p-1)/2} = -1$. Therefore, we have that $a = (-a)^{(p+1)/2}$ as $(p+1)/2$ is odd, which means $-a$ must also be a primitive root. Hence, a is a primitive root if and only if $-a$ is (interchanging their roles).
Now, let $p \equiv 3$ mod 4. If a is a primitive root, then $a^{(p-1)/2} = -1$ which gives $(-a)^{(p-1)/2} = 1$ as $(p-1)/2$ is odd. Then, the order of $-a$ is a divisor d of the odd number $(p-1)/2$. Then, $a^{2d} = (-a)^{2d} = 1$ which means $p-1$ divides $2d$; that is, $d = (p-1)/2$.
Conversely, let $-a$ have order $(p-1)/2$ and we claim a as order $p-1$ (when $p \equiv 3$ mod 4). Let d be the order of a. If d is odd, then $(-a)^d = -a^d = -1$ which gives, on raising to the $(p-1)/2$-th power (an odd power), we get $1 = (-a)^{(p-1)d/2} = (-1)^{(p-1)/2} = -1$, a contradiction. Hence the order d of a is even. Write it as $d = 2D$ where D divides $(p-1)/2$. So, $a^D = -1$ which gives $(-a)^D = 1$ as D is odd. Hence, $(p-1)/2$ divides D so that $p-1$ divides $2D = d$; so, $d = p-1$.

Exercise 6, Page 48, Chapter 4, I-R.
let $p = 2^n + 1 > 3$ be a prime. We will show that 3 is a primitive root mod p.
As $p-1$ is a power of 2, the order of 3 will be a power of 2 which means that 3 is a primitive root if, and only if, it is not a square. Once again, it can

be proved using QRL that 3 is not a square but, we will give another proof without QRL now. We will show that -3 is not a square which suffices since -1 is a square (as $p \equiv 1 \bmod 4$).
Suppose, if possible, $-3 \equiv b^2 \bmod p$. We may assume that b is odd as we may add multiples of p. Write $b = 2a + 1$ to get

$$-3 \equiv (2a+1)^2.$$

So, $4a^2 + 4a + 4 \equiv 0 \bmod p$. As p is odd, we get $a^2 + a + 1 \equiv 0 \bmod p$. This implies,

$$0 = a^3 - 1 = (a-1)(a^2 + a + 1) \equiv 0$$

but $a \not\equiv 1 \bmod p$ (else $3 \equiv 9$). Therefore, a has order 3 mod p which gives $p \equiv 1 \bmod 3$. This is a contradiction as a Fermat prime $2^n+1 > 3$ is 2 mod 3.

Exercise 7, Page 48, Chapter 4, I-R.
Let $p = 8t+3 > 3$ be a prime such that $q = (p-1)/2 = 4t+1$ is also prime. We show that 2 is a primitive root mod p.
As the divisors of $p-1$ are $1, 2, (p-1)/2, p-1$, the order of 2 is among $(p-1)/2$ and $p-1$ because they are not 1 or 2. To prove our contention, we need to check that $(p-1)/2$ is not the order (which is equivalent to 2 being not a square).
We will show that 2 is not a square mod p as $p \equiv 3 \bmod 8$.
Write each of the numbers $2, 4, 6, \cdots, p-1$ congruent to a unique integer with $|a| < p/2$. We will do it alternatively from the rightmost number to the leftmost one. Thus,

$$p - 1 \equiv (-1)^1.1;$$
$$2 \equiv (-1)^2.2;$$
$$p - 3 \equiv (-1)^3.3;$$
$$4 \equiv (-1)^4.4;$$
$$vdots$$

Multiplying them all out, we get

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv (-1)^{1+2+\cdots+(p-1)/2}\left(\frac{p-1}{2}\right)!$$

Cancelling off $\left(\frac{p-1}{2}\right)!$, we have

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \quad mod \quad p.$$

Our prime p is of the form $8k+3$ which means $2^{(p-1)/2} \equiv -1 \bmod p$. This proves 2 is not a square mod p and hence, it is a primitive root mod p as argued above.
We also mention in passing that we can prove this also using finite fields. Thus, we have proved the assertion without using QRL.

Exercise 8, Page 48, Chapter 4, I-R.
We show that a is a primitive root mod p (odd) if and only if $a^{(p-1)/q} \neq 1$ for every prime q dividing $p-1$.
Now a is NOT a primitive root if, and only if, $a^{(p-1)/d} \equiv 1 \bmod p$ for some $d > 1$. If this happens, then for any prime divisor q of d, write $d = qD$ and we get $a^{(p-1)/q} = (a^{(p-1)/d})^D = 1$. Converse is clear.

Exercise 9, Page 48, Chapter 4, I-R.
We will show that the product of all the primitive roots mod p is $-1)^{\phi(p-1)}$. Let a be a primitive root mod p. Then, the generators of the group $\mathbb{Z}_p^*$ are a^r as r varies over integers coprime to $p-1$. So, their product equals $a^{\sum_{(r,p-1)=1} r}$. For R coprime to $p-1$, $p-1-r$ is also coprime and is unequal to r when $p > 3$ (else $2r = p-1$ and so $r = (p-1)/2$ is coprime to $p-1$ which is impossible for $p > 3$). Hence, the product is a^s where $s = \frac{\phi(p-1)(p-1)}{2}$. So, $a^s = (-1)^{\phi(p-1)}$.