Comments on primitive roots

Review. $x \pmod n$ is a primitive root.

$\iff$ The (multiplicative) order of $x \pmod n$ is $\phi(n)$. (That is, the order is as large as possible.)

$\iff$ $x, x^2, \ldots, x^{\phi(n)}$ is a list of all invertible residues modulo n.

Example 155. Determine all primitive roots modulo 11.

Solution. Since $\phi(11) = 10$, the possible orders of residues modulo 11 are $1, 2, 5, 10$. Residues with order 10 are primitive roots. Our strategy is to find one primitive root and to use that to compute all primitive roots.

There is no good way of finding the first primitive root. We will just try the residues $2, 3, 5, 6, \ldots$ (why not 4?!)

We compute the order of $2 \pmod{11}$:

Since $2^2 = 4 \not\equiv 1$, $2^5 \equiv -1 \not\equiv 1 \pmod{11}$, we find that 2 has order 10. Hence, 2 is a primitive root.

Therefore, all other invertible residues are of the form 2^x. Recall that the order of $2^x \pmod{11}$ is $\frac{10}{\gcd(10, x)}$.

Hence, 2^x is a primitive root if and only if $\gcd(10, x) = 1$, which yields $x = 1, 3, 7, 9$.

In conclusion, the primitive roots modulo 11 are $2^1 = 2, 2^3 = 8, 2^7 \equiv 7, 2^9 \equiv 6$.

Comment. We don't need to check if 4 is a primitive root because $4 = 2^2$ (therefore, if 2 is not a primitive root then 4 could not possibly be a primitive root either).

Example 156. (extra) Determine all primitive roots modulo 22.

Solution. We proceed as in the previous example:

- Since $\phi(22) = 10$, the possible orders of residues modulo 22 are $1, 2, 5, 10$.
- We find one primitive root by trying residues $3, 5, \ldots$ (2 is out because it is not invertible modulo 22)
  Since $3^5 \equiv 1 \pmod{22}$, 3 is not a primitive root modulo 22.
  Since $5^5 \equiv 1 \pmod{22}$, 5 is not a primitive root modulo 22.
  Since $7^2 \not\equiv 1$, $7^5 \equiv -1 \not\equiv 1 \pmod{22}$, 7 is a primitive root modulo 22.
- $7^x \pmod{22}$ has order $\frac{10}{\gcd(10, x)}$. We have $\gcd(10, x) = 1$ for $x = 1, 3, 7, 9$.
- Hence, the primitive roots modulo 22 are $7^1 = 7, 7^3 \equiv 13, 7^7 \equiv 17, 7^9 \equiv 19$.

Proceeding as in the previous example, we obtain the following result.

Theorem 157. (number of primitive roots) Suppose there is a primitive root modulo n. Then there are $\phi(\phi(n))$ primitive roots modulo n.

Proof. Let x be a primitive root. It has order $\phi(n)$. All other invertible residues are of the form x^a.

Recall that x^a has order $\frac{\phi(n)}{\gcd(\phi(n), a)}$. This is $\phi(n)$ if and only if $\gcd(\phi(n), a) = 1$. There are $\phi(\phi(n))$ values a among $1, 2, \ldots, \phi(n)$, which are coprime to $\phi(n)$.

In conclusion, there are $\phi(\phi(n))$ primitive roots modulo n. □

Comment. Recall that, for instance, there is no primitive root modulo 15. That's why we needed the assumption that there should be a primitive root modulo n (which is the case if and only if n is of the form $1, 2, 4, p^k, 2p^k$ for some odd prime p).

In particular, since there are always primitive roots modulo primes, we have the following important case:

There are $\phi(\phi(p)) = \phi(p-1)$ primitive roots modulo a prime p.

Armin Straub
straub@southalabama.edu

Back to RSA

(RSA encryption)

- Bob chooses large random primes p, q.
- Bob chooses e, and then computes d such that $de \equiv 1 \pmod{(p-1)(q-1)}$.
- Bob makes $N = pq$ and e public. His (secret) private key is d.
- Alice encrypts $c = m^e \pmod{N}$.
- Bob decrypts $m = c^d \pmod{N}$.

Does decryption always work? What Bob computes is $c^d \equiv (m^e)^d = m^{de} \pmod{N}$. It follows from Euler's theorem and $de \equiv 1 \pmod{\phi(N)}$ that $m^{de} \equiv m \pmod{\phi(N)}$ for all invertible residues m. That this actually works for all residues can be seen from the Chinese Remainder Theorem (see Theorem 158 below).

Is that really secure? Well, if implemented correctly (we will discuss potential issues), RSA has a good track record of being secure. Next class, we will actually prove that finding the secret key d is as difficult as factoring N (which is believed, but has not been proven, to be hard). On the other hand, it remains an important open problem whether knowing d is actually necessary to decrypt a given message.

Comment. The $(p-1)(q-1)$ in the generation of d can be replaced with $\operatorname{lcm}(p-1, q-1)$. This will be illustrated in Example 162.

Theorem 158. Let $N = pq$ and d, e be as in RSA. Then, for any m, $m \equiv m^{de} \pmod{N}$.

Comment. Using Euler's theorem, this follows immediately for residues m which are invertible modulo N. However, it then becomes tricky to argue what happens if m is a multiple of p or q.

Proof. By the CRT, we have $m \equiv m^{de} \pmod{N}$ if and only if $m \equiv m^{de} \pmod{p}$ and $m \equiv m^{de} \pmod{q}$.
Since $de \equiv 1 \pmod{(p-1)(q-1)}$, we also have $de \equiv 1 \pmod{p-1}$. By little Fermat, it follows that $m^{de} \equiv m \pmod{p}$ for all $m \not\equiv 0 \pmod{p}$. On the other hand, if $m \equiv 0 \pmod{p}$, then this is obviously true. Thus, $m \equiv m^{de} \pmod{p}$ for all m. Likewise, modulo q. □

Example 159. Bob's public RSA key is $N = 33$, $e = 3$.

(a) Encrypt the message $m = 4$ and send it to Bob.

(b) Determine Bob's secret private key d.

(c) You intercept the message $c = 31$ from Alice to Bob. Decrypt it using the secret key.

Solution.

(a) The ciphertext is $c = m^e \pmod{N}$. Here, $c \equiv 4^3 = 64 \equiv 31 \pmod{33}$. Hence, $c = 31$.

(b) $N = 3 \cdot 11$, so that $\phi(N) = 2 \cdot 10 = 20$.
To find d, we need to compute $e^{-1} \pmod{20}$. Since the numbers are so simple we see $3^{-1} \equiv 7 \pmod{20}$.
Hence, $d = 7$.

(c) We need to compute $m = c^d \pmod{N}$, that is, $m = 31^7 \equiv (-2)^7 \equiv 4 \pmod{33}$.
That is, $m = 4$ (as we already knew from the first part).

Example 160. For his public RSA key, Bob needs to select p, q and e. Which of these must be chosen randomly?

Solution. The primes p and q must be chosen randomly. Anything that makes these primes more predictable, makes it easier for an attacker to get her hands on them [in which case, the secret key d is trivial to compute].
On the other hand, e does not need to be chosen at random. In fact, knowing any pair e, d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$ would allow us to factor $N = pq$ (and thus break RSA). We'll prove that later.