## Facts about Finite Fields

1. In any finite field, in particular in the field $\mathbf{Z}_p$ where $p$ is a prime integer, there exists a *primitive element* $\alpha$ such that the successive powers of $\alpha$ generate all nonzero elements of the field. In other words, $\alpha$ satisfies:

$$\alpha^{p-1} = 1 \ ;$$

$$\alpha^j \neq 1 \ \text{ for } \ 0 < j < p-1 \ .$$

   We also say that $\alpha$ is an *element of order* $p-1$, and note that $\alpha$ is a *primitive root of* $x^{p-1} - 1 = 0$ .

   Therefore, the elements of the finite field $\mathbf{Z}_p$ can be represented by

$$\{0\} \cup \{\alpha^j, j = 0, 1, \ldots, p-2\} \ .$$

   (It is always the case that $a^{p-1} = 1$ for any nonzero element $a \in \mathbf{Z}_p$ .)

2. An element $\omega \in \mathbf{Z}_p$ is called a *primitive* $n^{th}$ *root of unity* if

$$\omega^n = 1 \ ;$$

$$\omega^k \neq 1 \ \text{ for } \ 0 < k < n \ .$$

   In other words, $\omega$ is a root of $x^n - 1 = 0$ and the powers of $\omega$ generate the $n$ distinct roots of $x^n - 1 = 0$.

   We say that $\omega$ is an *element of order* $n$.

3. If $n \mid (p-1)$ then in the finite field $\mathbf{Z}_p$ there exists an element $\omega$ of order $n$ (i.e., there exists a primitive $n^{th}$ root of unity).

   **Proof**: Let $\alpha$ be a primitive element in $\mathbf{Z}_p$ and choose

$$\omega = \alpha^{(p-1)/n} \ .$$

   Then $\omega^n = \alpha^{p-1} = 1$ in $\mathbf{Z}_p$ . Moreover, if $0 < k < n$ then

$$\omega^k = \alpha^{k(p-1)/n} = \alpha^j \ \text{ where } \ 0 < j < p-1 \ .$$

   I.e., $\omega^k \neq 1 \ \text{ for } \ 0 < k < n$ , from Fact 1.

4. How can we calculate an element $\omega$ of order $n$ in $\mathbf{Z}_p$ ?

   We might consider a **brute force approach**: Try $\omega = 2, 3, 4, \ldots$ until we find an $\omega$ such that $\omega^n = 1$ , and $\omega^k \neq 1$ for $0 < k < n$ .

   However, for a finite field the size of interest on Assignment 2 (where $p$ is an 8-digit prime), you will find that you can compute for a very very long time and you will still not have found such an $\omega$.

   **Smart approach**: Define $\omega$ as in the Proof of Fact 3 above.

   This raises the question: But how can we compute a primitive element $\alpha$ for the finite field $\mathbf{Z}_p$ ?

5. How can we calculate a primitive element $\alpha \in \mathbf{Z}_p$ ?

   This time, we have no method other than a "brute force approach": Try $\alpha = 2, 3, 4, \ldots$ until we find an $\alpha$ such that

   $$\alpha^{p-1} = 1 \ , \text{ and } \alpha^j \neq 1 \text{ for } 0 < j < p-1 \ .$$

   This is a practical method because it turns out that about 30% of the elements in a finite field $\mathbf{Z}_p$ are primitive elements. (See Fact 6 below.) So by the time we have tried about three or four values for $\alpha$, we will probably have found a primitive element!

   **Note 1**: When doing powering operations, in order not to be hopelessly inefficient we need to be using the "binary powering method". (See page 117 of the textbook.) In Maple, it is just a matter of being sure to use the inert power operator and then the application of the `mod` operator in Maple will do the powering efficiently.

   I.e., we must write `a &^ b mod p` and not `a ^ b mod p` (see the help page `?mod` in Maple).

   Of course, all arithmetic operations being discussed here are to be done `mod p` because we are doing arithmetic in the field $\mathbf{Z}_p$ .

   **Note 2**: When searching for a primitive element $\alpha \in \mathbf{Z}_p$ by the "brute force approach", there is no need to check that $\alpha^{p-1} = 1$ because, as noted in Fact 1 above, it is always the case that $a^{p-1} = 1$ for *any* nonzero element $a \in \mathbf{Z}_p$ .

**Note 3**: It is also not necessary to check all the powers less than $p-1$ to see that they differ from 1. Rather, the following theorem makes our method much more efficient.

**Theorem**: The element $\alpha$ is a primitive element in $\mathbf{Z}_p$ if and only if

$$\alpha^{(p-1)/q} \neq 1 \pmod{p}$$

for each prime factor $q$ of $p-1$ .

(Hence why you were asked in Assignment 2, Question 5 to compute the prime factorization of $p-1$ .)

6. There are lots of primitive elements in $\mathbf{Z}_p$ .

   **Theorem**: The number of primitive elements in $\mathbf{Z}_p$ is $\phi(p-1)$ where $\phi(a)$ is the "Euler $\phi$ function" (i.e., the number of integers less than $a$ which are relatively prime to $a$).

   We learn from Number Theory that $\phi(p-1)$ is approximately equal to $\frac{3}{\pi^2}(p-1)$ or about .30 $(p-1)$. I.e., approximately 30% of the elements in $\mathbf{Z}_p$ are primitive elements.