MA542. Yuhua Zhu.

Prob16. For a finite field F, $a \in F$ a generator of F.
$\Leftrightarrow \forall 0 \neq f \in F$, $f = a^n$, some $n \in \mathbb{Z}$.

1). Find a generator of $\mathbb{Z}_7$.

$3^2 \equiv 2 \bmod 7$.

$3^3 \equiv 6 \bmod 7$.

$3^4 \equiv 4 \bmod 7$.

$3^5 \equiv 5 \bmod 7$.

$3^6 \equiv 1 \bmod 7$.

$3 \equiv 3 \bmod 7$.

$\therefore 3$ is a generator of $\mathbb{Z}_7$.

ok

2). How many generators does $\mathbb{Z}_{17}$ have.

$\because (\mathbb{Z}_{17}^*, \times) \cong C_{16}$. (by Corollary 26: the multiplicative grp of a finite field is cyclic).

$\because \forall 1 \le n \le 16$, $\gcd(n, 16) = 1 \Leftrightarrow \langle n \rangle = C_{16}$, $\because 16 = 2^4$.

According to Euler function # of such $n = 16 \times (1 - \frac{1}{2}) = 8$.

(pf: "$\Rightarrow$" if $in \equiv jn \bmod 16$, for $1 \le i < j \le 16$. $\Rightarrow 16 \mid (j-i)n$. $\Rightarrow \times$.

$\therefore$ for $\forall 1 \le i \ne j \le 16$, $in \ne jn \Rightarrow \langle n \rangle = C_{16}$.

"$\Leftarrow$" if $\gcd(n, 16) \ne 1$, $\exists d > 1$, $d \mid n$, $d \mid 16$.

$\therefore n = (1 + \frac{16}{d}) n$. $\because 1 < 1 + \frac{16}{d} < 16$. $\therefore |\langle n \rangle| < 16$. $\Rightarrow \times$.)

$\therefore$ there are 8 generators in $\mathbb{Z}_{17}$.

3). How many generators does $\mathbb{Z}_{31}$ have?

$\because (\mathbb{Z}_{31}^*, \cdot) \cong C_{30}$, $30 = 2 \times 3 \times 5$.

$\varphi(30) = 30 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{3}) \times (1 - \frac{1}{5}) = 8$.

$\therefore$ there are 8 generators in $\mathbb{Z}_{31}$.

Math 542 Exercise 16

Joe Timmerman

February 26 , 2014

All of this was done using pretty ugly code I wrote in Java, which I'll attach. I've pasted the output of my program for each part.

a) Find a generator of $\mathbb{Z}_7$

```
n = 7
Generators are: 3, 5,
Total number of generators: 2
```

b) How many generators does $\mathbb{Z}_{17}$ have?

```
n = 17
Generators are: 3, 5, 6, 7, 10, 11, 12, 14,
Total number of generators: 8
```

c) How many generators does $\mathbb{Z}_{31}$ have?

```
n = 31
Generators are: 3, 11, 12, 13, 17, 21, 22, 24,
Total number of generators: 8
```

```java
public class FindGenerators {



    public static void main(String[] args) {

        int n = 31;
        System.out.println("n = " + n);
        boolean[] isGenerator = new boolean[n];

        for(int i = 1; i < n; i++) {
            boolean[] elements = new boolean[n];
            for(int k = 0; k < n; k++) {
                elements[k] = false;
            }
            for(int j = 1; j < n; j++) {
                BigInteger currentInt = new BigInteger(String.valueOf(i));
                for(int l = 1; l <  1000; l++) {

                    if(currentInt.modPow(BigInteger.valueOf(l),
                            BigInteger.valueOf(n)).equals(BigInteger.valueOf(j)))   {
                        elements[j] = true;
                    }
                }
            }
            boolean isGen = true;
            for(int m = 1; m < n; m++) {
                if(elements[m] == false) {
                    isGen = false;
                }
            }
            isGenerator[i] = isGen;
        }
        int count = 0;
        System.out.print("Generators are: ");
        for(int a = 1; a < n; a++) {

            if(isGenerator[a]) {
                System.out.print(a + ", ");
                count++;
            }
        }
        System.out.println("\nTotal number of generators: " + count);
    }
}
```