

Aufgabe 36

Die Restklassen zum Primem Modul 2333 mit der Ordnung 22 sind :
213, 311, 701, 862, 1183, 1265, 1291, 1414, 2108 und 2318.

Die Restklassen zum primen Modul 2333 mit der Ordnung 53 sind :
61, 79, 153, 187, 262, 279, 341, 422, 425, 430, 466, 485, 567, 593, 615, 646, 676,
680, 688, 693, 747, 775, 776, 821, 847, 852, 913, 984, 987, 1044, 1088, 1178, 1240,
1276, 1308, 1388, 1575, 1589, 1699, 1819, 1868, 1882, 1925, 1964, 1984, 2034,
2041, 2042, 2075, 2078, 2137 und 2307.

Dieses Ergebnis wurde per Perl-Skript ermittelt :

```
./uebung10.pl 36
```

Das Perlskript geht nach Korollar 6.1.4 vor; es testet hierfür für $g \in \{2, \dots, 2333\}$ ob gilt $g^m = 1 \pmod{2333}$ und $g^{\frac{m}{q}} \neq 1 \pmod{2333}$ für alle $q \in P_m$ wobei P_m die Primteiler von m sind. Dies jeweils mit $m = 22$ bzw. $m = 53$.

Aufgabe 37

- (a) Laut Satz 6.1.2 gibt es in \mathbb{Z}_p^* genau $\Phi(p-1)$ Primitivwurzeln \pmod{p} . Nach Aufgabenstellung ist $q = \frac{p-1}{2}$, womit auch die beiden Primteiler von $p-1$ gegeben sind (nämlich 2 und $\frac{p-1}{2}$). $\Phi(p-1)$ ist somit $\Phi(2) \cdot \Phi(q)$, also $1 \cdot (q-1)$. Die Erfolgswahrscheinlichkeit, zufällig eine Primitivwurzel zu p in $\{2, \dots, p-1\}$ zu finden ist also $\frac{q-1}{|\{2, \dots, p-1\}|} = \frac{q-1}{p-2}$, was bei grossen Zahlen bei etwa $\frac{1}{2}$ liegt.
- (b) `mod_exp` benötigt je Durchlauf die Anzahl der 1-Bits in Binärdarstellung des Exponenten an Multiplikationen. Um nach dem im Skript auf S. 90 beschriebenen Verfahren darauf zu testen, ob a eine Primitivwurzel von p ist, wird `mod_exp` mit den Exponenten 2 und q aufgerufen; somit werden je Test (unter Annahme dass die Hälfte aller Bits in q gesetzt sind) $\frac{q}{2} + 1$ Multiplikationen benötigt. Nimmt man nun die in (a) ermittelte Erfolgswahrscheinlichkeit von $\frac{1}{2}$ an, so wird durchschnittlich nur ein Test benötigt (sofern man 'durchschnittlich' also 'in 50% der Fälle korrekt' annimmt; damit werden also durchschnittlich $\frac{q}{2} + 1$ Multiplikationen benötigt, um eine Primitivwurzel zu finden.

Ein Perl-Skript verifiziert dieses Ergebnis :

```
./uebung10.pl 37
```

lässt 5000 Tests dieser Art durchlaufen (mit der Primzahl 863, wobei $\frac{863-1}{2} = 431$ auch prim ist); 2519 dieser Tests verliefen positiv, was in etwa dem erwarteten Ergebnis entspricht.

Anhang 36-37

```
#!/usr/local/bin/perl
use strict; no strict 'refs'; use Math::BigInt;

sub modexp {
    my ($a, $b, $n) = @_;
    my $d = new Math::BigInt (1);
    my @b = split //, sprintf "%0b", $b;
    for my $i (0..@b-1) {
        $d = $d*$d % $n;
        $d = $d*$a % $n if $b[$i]
    }
    $d
}

sub k614 {
    my ($n, $m, @pt) = @_; my %r;
    for my $i (@pt) {
        modexp ($_, $m, $n) == 1 and modexp ($_, $m/$i, $n) != 1 and $r{$_}++ for 2..$n
    }
    my @r = sort { $a <=> $b } map { $r{$_} == @pt ? $_ : () } keys %r;
    print scalar @r, "\n";
    @r;
}

sub prob36 {
    map { print join (" ", k614 ( map { new Math::BigInt ($_) } @{$_})), "\n" }
        [2333, 53, 53], [2333, 22, 2, 11]
}

sub prob37 {
    my $p = 863; my $r;
    for (1..5000) {
        my $a = 1 + int rand $p-1;
        modexp ($a, 2, $p) != 1 and modexp ($a, 431, $p) != 1 and $r++
    }
    print $r, "\n";
}

&{'prob'.$ARGV[0]} (splice @ARGV,1)
```