

This note relates to Problem 4.1(e) of Problem Set 4 for 6.857 (Fall 2004), which asked:

Estimate the length of the longest safe prime $p = 2q + 1$ you would expect to find among the first million digits of e such that 3 is a generator modulo p .

(A safe prime is a prime p of the form $2q + 1$ where q is also prime.)

I was surprised by the answer, so the homework was “buggy.” This note explains the correct answer, as well as the intended answer.

We explain the intended answer first, starting with the related problem of estimating the density of safe primes.

For a given large integer q , the density of primes near q can be estimated as $1/\ln(q)$, by the Prime Number Theorem. Thus, the “probability” that a large randomly chosen integer q is prime can be estimated as $1/\ln(q)$. For such a given q , the probability that p is prime as well (where $p = 2q + 1$), can be estimated as $2/\ln p$; the factor of 2 arises since p is necessarily odd. Assume that p and q are large, so that $\ln(p)$ and $\ln(q)$ are good relative approximations for each other. Using the probability theorem that says $\text{Prob}(A \text{ and } B) = \text{Prob}(A)\text{Prob}(B|A)$, we have that the “probability that a given large integer p is a safe prime” can be estimated as $2/\ln^2(p)$. (Here we make the assumption that the probability of p being prime is independent of whether q is prime.) Thus, the longest safe prime among the first million digits of e should be about the largest k such that

$$10^6 \cdot (2/\ln^2(10^k)) = 1 ,$$

which solves approximately to

$$k = 614$$

Now, turning to the question of 3 being a generator.

For any prime p , an element g is a generator if it has order $p - 1$. That is, it must not have order d for any divisor d of $p - 1$, where d is strictly less than $p - 1$.

When p is a safe prime, $p - 1 = 2q$, so that the only possible orders for an element g are 1, 2, q , and $2q$.

There is only one element of order 1, which is the element 1 itself.

There is only one element of order 2, which is the element $-1 = p - 1$.

There are q elements of order either 1 or q ; these are the squares (quadratic residues) modulo p , since for any quadratic residue $b = a^2$:

$$b^q = (a^2)^q = a^{2q} = a^{p-1} = 1 \pmod{p} .$$

Since there are only q squares modulo p , it follows that b is a square modulo p if and only if $b^q = 1 \pmod{p}$.

Thus g is a generator if it is not a square and also not equal to -1 modulo p , when p is a safe prime. There should be $q - 1$ such generators modulo $p = 2q + 1$.

(For the above we note that if $p = 2q + 1$ is a safe prime, then (-1) can not be a square modulo p , since $(-1)^q = -1 \pmod{p}$, assuming q odd. Of course, 4 is a square modulo 5.)

Example: When $p = 7$, the squares are 1, 4, and 2, so the generators are 3 and 5.

It was our expectation that 3 would be a generator modulo p approximately half the time as you vary the choice of p ; more precisely, we might expect 3 to be a generator approximately $(q - 1)/(p - 1) \approx 1/2$ of the time (as you vary the choice of the safe prime p), since there are $q - 1$ generators modulo such a prime p , and there are $p - 1$ elements in Z_p^* other than -1 to choose “3” from.

Indeed, if we had asked for 5 rather than 3 as a generator, such an crude analysis would have given us the right answer.

However, there was a surprise in store for 3, as the constraint that p be a safe prime makes it almost (but not quite) impossible that 3 be a generator modulo p . Indeed, the only safe primes for which 3 is a generator are 5 and 7.

Let $\left(\frac{a}{p}\right)$ denote 1 if a (non-zero mod p) is a quadratic residue (square) modulo p , and -1 otherwise. This is known as the “quadratic residuosity symbol”.

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

The “law of quadratic residuosity” states that if p and r are two odd primes, then

$$\left(\frac{p}{r}\right) \left(\frac{r}{p}\right) = (-1)^{\frac{p-1}{2} \frac{r-1}{2}}.$$

(This is not so easy to prove!)

Taking $r = 3$ and $p = 2q + 1$, and assuming that $\left(\frac{3}{p}\right) = -1$ since we want 3 to be a generator modulo p , we get that

$$\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right) (-1)^{\frac{p-1}{2} \frac{r-1}{2}}.$$

$$\left(\frac{p}{3}\right) = (-1)(-1)^{q \frac{3-1}{2}}.$$

$$\left(\frac{p}{3}\right) = (-1)(-1)^q.$$

If q is odd, then p must be a square modulo 3, which means that $p = 1 \pmod{3}$. Since $q = 2s + 1$ for some s , we also know that $p = 2q + 1 = 4s + 3$, so $p = 3 \pmod{4}$.

But if $p = 1 \pmod{3}$ and $p = 3 \pmod{4}$, then $p = 7 \pmod{12}$. But then $q = (p - 1)/2$ must satisfy $q = 3 \pmod{6}$. The only prime p satisfying this condition is $q = 3$, yielding $p = 7$. Considering the possibility that q might be an even prime yields the other possibility $p = 5$, for which 3 is indeed a generator.

Thus, there are no safe primes other than 5 and 7 for which 3 is a generator.

Number of primes less than 10000	=	1229
Number of primes less than 10000 with generator 2	=	470
Number of primes less than 10000 with generator 3	=	476

Number of primes less than 10000 with generator 4 =	0
Number of primes less than 10000 with generator 5 =	491
Number of primes less than 10000 with generator 6 =	470
Number of primes less than 10000 with generator 7 =	464

Number of safe primes less than 10000 =	115
Number of safe primes less than 10000 with generator 2 =	53
Number of safe primes less than 10000 with generator 3 =	2
Number of safe primes less than 10000 with generator 4 =	0
Number of safe primes less than 10000 with generator 5 =	72
Number of safe primes less than 10000 with generator 6 =	52
Number of safe primes less than 10000 with generator 7 =	47

Prime: 2
Generators less than 20:

Prime: 3
Generators less than 20: 2

Prime: 5 (SAFE)
Generators less than 20: 2 3

Prime: 7 (SAFE)
Generators less than 20: 3 5

Prime: 11 (SAFE)
Generators less than 20: 2 6 7 8

Prime: 13
Generators less than 20: 2 6 7 11

Prime: 17
Generators less than 20: 3 5 6 7 10 11 12 14

Prime: 19
Generators less than 20: 2 3 10 13 14 15

Prime: 23 (SAFE)
Generators less than 20: 5 7 10 11 14 15 17 19

Prime: 29
Generators less than 20: 2 3 8 10 11 14 15 18 19

Prime: 31
Generators less than 20: 3 11 12 13 17

Prime: 37
Generators less than 20: 2 5 13 15 17 18 19

Prime: 41
Generators less than 20: 6 7 11 12 13 15 17 19

Prime: 43
Generators less than 20: 3 5 12 18 19

Prime: 47 (SAFE)
Generators less than 20: 5 10 11 13 15 19

Prime: 53
Generators less than 20: 2 3 5 8 12 14 18 19

Prime: 59 (SAFE)
Generators less than 20: 2 6 8 10 11 13 14 18

Prime: 61
Generators less than 20: 2 6 7 10 17 18

Prime: 67
Generators less than 20: 2 7 11 12 13 18

Prime: 71
Generators less than 20: 7 11 13

Prime: 73
Generators less than 20: 5 11 13 14 15

Prime: 79
Generators less than 20: 3 6 7

Prime: 83 (SAFE)
Generators less than 20: 2 5 6 8 13 14 15 18 19

Prime: 89
Generators less than 20: 3 6 7 13 14 15 19

Prime: 97
Generators less than 20: 5 7 10 13 14 15 17

Prime: 101
Generators less than 20: 2 3 7 8 11 12 15 18

Prime: 103
Generators less than 20: 5 6 11 12

Prime: 107 (SAFE)
Generators less than 20: 2 5 6 7 8 15 17 18

Prime: 109
Generators less than 20: 6 10 11 13 14 18

Prime: 113
Generators less than 20: 3 5 6 10 12 17 19

Prime: 127
Generators less than 20: 3 6 7 12 14

Prime: 131
Generators less than 20: 2 6 8 10 14 17

Prime: 137
Generators less than 20: 3 5 6 12 13

Prime: 139
Generators less than 20: 2 3 12 15 17 18 19

Prime: 149
Generators less than 20: 2 3 8 10 11 12 13 14 15 18

Prime: 151
Generators less than 20: 6 7 12 13 14 15

Prime: 157
Generators less than 20: 5 6 15 18

Prime: 163
Generators less than 20: 2 3 7 11 12 18 19

Prime: 167 (SAFE)
Generators less than 20: 5 10 13 15 17

Prime: 173
Generators less than 20: 2 3 5 7 8 11 12 17 18 19

Prime: 179 (SAFE)
Generators less than 20: 2 6 7 8 10 11 18

Prime: 181

Generators less than 20: 2 10 18

Prime: 191

Generators less than 20: 19

Prime: 193

Generators less than 20: 5 10 15 17 19

Prime: 197

Generators less than 20: 2 3 5 8 11 12 13 17 18

Prime: 199

Generators less than 20: 3 6 15