

Example

Let $n = 8$ and $p = 11$

Then

0		
$\text{mod}(2, 11)$	=	1
1		
$\text{mod}(2, 11)$	=	2
2		
$\text{mod}(2, 11)$	=	4
3		
$\text{mod}(2, 11)$	=	8
4		
$\text{mod}(2, 11)$	=	5
5		
$\text{mod}(2, 11)$	=	10
6		
$\text{mod}(2, 11)$	=	9
7		
$\text{mod}(2, 11)$	=	7

This yields a table of the form

remainder	bit position
0	--
1	0
2	1
3	--
4	2
5	4
6	--
7	7
8	3
9	6
10	5

Good Divisors

The divisor p should be as small as possible in order to minimize the length of the table. Since the divisor must generate n distinct remainders, the divisor will certainly need to be at least n . A remainder of zero, however, can occur only if the divisor is a power of 2. If the divisor is a small power of 2, say 2^j for $j < n-1$, it will not generate n distinct remainders; if the divisor is a larger power of 2, the correspondence table is either 2^{n-1} or 2^n in length. We can thus rule out zero as a remainder value, so the divisor must be at least one more than the word length. This bound is in fact achieved for some word lengths.

Let $R(p)$ be the number of distinct remainders p generates when divided into successively higher powers of 2. The distinct remainders all occur for the $R(p)$ lowest powers of 2. Only odd p are interesting and the following table gives $R(p)$ for odd p between 1 and 21.

p	$R(p)$	p	$R(p)$
1	1	13	12
3	2	15	4
5	4	17	8
7	3	19	18
9	6	21	6
11	10		

This table shows that 7, 15, 17 and 21 are useless divisors because there are smaller divisors which generate a larger number of distinct remainders. If we limit our attention to p such that $p > p' \Rightarrow R(p) > R(p')$, we obtain the following table of useful divisors for $p < 100$.

p	R(p)	p	R(p)
1	1	29	28
3	2	37	36
5	4	53	52
9	6	59	58
11	10	61	60
13	12	67	66
19	18	83	82
25	20		

Notice that 9 and 25 are useful divisors even though they generate only 6 and 20 remainders, respectively.

Determination of R(p)

If p is odd, the remainders

$$\begin{aligned} & 0 \\ & \text{mod}(2^0, p) \\ & 1 \\ & \text{mod}(2^1, p) \\ & \cdot \\ & \cdot \\ & \cdot \end{aligned}$$

will be between 1 and p-1 inclusive. At some power of 2, say 2^t , there will be a repeated remainder, so that for some $k < t$, $2^k = 2^t \pmod p$.

$$\begin{aligned} \text{Since } 2^{t+1} &= 2^{k+1} \pmod p \\ \text{and } 2^{t+2} &= 2^{k+2} \pmod p \end{aligned}$$

\cdot
 \cdot
 \cdot
etc.

all of the distinct remainders occur for $2^0 \dots 2^{t-1}$. Therefore, $R(p)=t$.

Next we show that

$$2^{R(p)} = 1 \pmod p$$

We already know that $2^{R(p)-k} = 2^k \pmod p$

for some $0 < k < R(p)$. Let $j = R(p) - k$ so $0 < j < R(p)$. Then

$$2^{k+j} = 2^k \pmod p$$

or $2^j \cdot 2^k = 2^k \pmod p$

or $(2^j - 1) \cdot 2^k = 0 \pmod p$

Now p does not divide 2^k because p is odd, so p must divide $2^j - 1$. Thus

$$2^j - 1 = 0 \pmod p$$

$$2^j = 1 \pmod p$$

Since j is greater than 0 by hypothesis and since there is no k other than 0 less than $R(p)$ such that

$$2^k = 2^0 \pmod p,$$

we must have $j = R(p)$, or $2^{R(p)} = 1 \pmod p$.

We have thus shown that for odd p , the remainders $\text{mod}(2^k, p)$ are unique for $k = 0, 1, \dots, R(p) - 1$ and then repeat exactly, beginning with

$$2^{R(p)} = 1 \pmod p.$$

We now consider even p . Let

$$p = p' \cdot 2^q,$$

where p' is odd. For $k < q$, $\text{mod}(2^k, p)$ is clearly just 2^k because $2^k < p$.

For $k \geq q$,

$$\text{mod}(2^k, p) = 2^q \cdot \text{mod}(2^{k-q}, p').$$

From this we can see that the sequence of remainders will have an initial segment of $1, 2, \dots, 2^{q-1}$ of length q , and repeating segments of length $R(p')$. Therefore, $R(p) = q + R(p')$. Since we normally expect

$$R(p) \sim p,$$

even p generally will not be useful.

I don't know of a direct way of choosing a p for a given n , but the previous table was generated from the following Fortran program run under the SEX system at UCLA.

```

0          CALL IASSGN('OC ',56)
1          FORMAT(I3,I5)
           M=0
           DO 100 K=1,100,2
           K=1
           L=0
20         L=L+1
           N=MOD(2*N,K)
           IF(N.GT.1) GO TO 20
           IF(L.LE.M) GO TO 100
           M=L
           WRITE(56,1)K,L
100        CONTINUE
           STOP
           END

```

Fortran program to computer useful divisors

In the program, K takes on trial values of p , N takes on the values of the successive remainders, L counts up to $R(p)$, and M remembers the previous largest $R(p)$. Execution is quite speedy.

Results from Number Theory

The quantity referred to above as $R(p)$ is usually written Ord_2 and is read "the order of 2 mod p ". The maximum value of Ord_2 is given by Euler's phi-function, sometimes called the totient. The totient of a positive integer p is the number of integers less than p which are relatively prime to p . The totient is easy to compute from a representation of p as a product of primes:

$$\text{Let } p = p_1^{n_1} * p_2^{n_2} \dots p_k^{n_k}$$

where the p_i are distinct primes. Then

$$\text{phi}(p) = (p_1 - 1) * p_1^{n_1 - 1} * (p_2 - 1) * p_2^{n_2 - 1} \dots (p_k - 1) * p_k^{n_k - 1}$$

If p is prime, the totient of p is simply

$$\text{phi}(p) = p-1.$$

If p is not prime, the totient is smaller.

If a is relatively prime to p , then Euler's generalization of Fermat's theorem states

$$a^{\text{phi}(p)} = 1 \text{ mod } p.$$

It is this theorem which places an upper bound Ord_2 , because Ord_2 is the smallest value such that

$$2^{\text{Ord}_2} = 1 \text{ mod } p$$

Moreover it is always true that $\text{phi}(p)$ is divisible by Ord_2 .

Acknowledgements

Bob Kahn read an early draft and made many comments which improved the exposition. Alex Hurwitz assured me that a search technique is necessary to compute $R(p)$, and supplied the names for the quantities and theorems I uncovered.

[This RFC was put into machine readable form for entry]
[into the online RFC archives by Guillaume Lahaye and]
[John Hewes 6/97]

