Problem 40 Solution

Eric Brier

No Institute Given

1 A equivalent condition

In this first section, we shall exhibit a great simplification of Crump's equation.

Proposition 1. *Crump's equation is equivalent to*

$$2^{zp} \equiv 2^z \ mod\ 2zp$$

Proof. We have $n = 2^{zp} + 1$. This means that $2^{zp} \equiv -1 \bmod n$, which implies that $2^{2zp} \equiv 1 \bmod n$. The multiplicative order o of 2 modulo n must divide $2zp$. Furthermore, $1 < 2^a < n$ when $0 < a \leq zp$, which shows that $o > zp$. The consequence of this is that $o = 2zp$. Crump's equation is of the form $2^\alpha \equiv 2^\beta \bmod n$. By definition of multiplicative order, this is equivalent to $\alpha \equiv \beta \bmod o$. Replacing the exponents by their values, one gets:

$$2^{zp} \equiv 2^z \bmod 2zp$$

□

2 Counterexample of second question

Using the previous proposition, one can easily verify that if $p = 53$ and $z = 14$, we have $p \equiv 1 \bmod (z-1)$ but:

$$\begin{aligned} 2^{zp} &\equiv 1332 \mod 2zp \\ 2^z &\equiv 60 \mod 2zp \end{aligned}$$

3 Solving Crump's Equation

Lets fix the integer z and let q be an odd prime factor of z. One can then write $z = q^\alpha m$ with m coprime to q. We are now dealing with equation

$$\mathcal{E}_q : 2^{zp} \equiv 2^z \bmod q^\alpha$$

We denote o_{q^α} the multiplicative order of 2 modulo q^α and o_q the multiplicative order of 2 modulo q. We have $o_{q^\alpha} = q^\beta o_q$ with $\beta \leq \alpha - 1$. Equation $\mathcal{E}_q$ is then equivalent to:

$$\begin{aligned} zp \equiv p \bmod o_{q^\alpha} &\Leftrightarrow o_{q^\alpha} \mid z(p-1) \\ &\Leftrightarrow o_q q^\beta \mid q^\alpha m(p-1) \\ &\Leftrightarrow o_q \mid m(p-1) \\ &\Leftrightarrow u_q \mid (p-1) \text{ with } u_q = \tfrac{o_q}{gcd(o_q, m)} \end{aligned}$$

The equation $\mathcal{E}_{q=p}$ is naturally satisfied by Fermat's Little Theorem. It remains to deal with the case $q = 2$, this case is also naturally satisfied. Crump's Equation is equivalent to the conjonction of all $\mathcal{E}_q$ for q dividing z, i.e. $\forall q, u_q|(p-1)$. Let's denote by $u(z)$ the least common multiple of $u(q)$ for all prime q dividing z. We have proved along the way:

Proposition 2. *With previous definitions, Crump's Equation is equivalent to:*

$$u(z)|p-1$$

One can notice that a divisibility condition is the correct answer to Crump's Equation but the correct number that has to divide $p-1$ is $u(z)$, which does not always divide $z-1$.

Computing $u(z)$ is not a difficult task as long as factoring z is easy. An interesting corollary of previous proposition is that Crump's Equation is satisfied for all prime p when $u(z) \in \{1, 2\}$. The following table gives the first values of function u:

$u(1) = 1$	$u(2) = 1$	$u(3) = 2$	$u(4) = 1$	$u(5) = 4$
$u(6) = 2$	$u(7) = 6$	$u(8) = 1$	$u(9) = 2$	$u(10) = 1$
$u(11) = 10$	$u(12) = 1$	$u(13) = 12$	$u(14) = 3$	$u(15) = 4$
$u(16) = 1$	$u(17) = 8$	$u(18) = 1$	$u(19) = 18$	$u(20) = 1$
$u(21) = 2$	$u(22) = 5$	$u(23) = 22$	$u(24) = 1$	$u(25) = 4$

The values in this table, combined with the above corollary, show that Crump's Equation is satisfied for all prime p when $z \leq 4$ but also for many other values: 8, 10, 12, 16, 18, 20, 21, 24.