Some Illustrations of Pollard's Rho Method

The Maple procedure rho(n,c,x0) implements Pollard's rho algorithm to find a proper factor of n, using iteration function $f(x) = x^2 + c$ starting with seed $x0$. It returns a proper factor of n if the algorithm succeeds, and returns 0 if it fails.

(1) rho(6557,1,2)=79 giving factorisation $6557 = 79 \times 83$.

i	$x = x_i$	x_{2i-1}	$y = x_{2i}$	$\lvert y - x \rvert$	$\gcd(y - x, n)$
	2		2		
1	5	5	26	21	1
2	26	677	5897	5871	1
3	677	2839	1369	692	1
4	5897	5417	1315	4582	79

(2) rho(7807,1,2)=37 giving factorisation $7807 = 37 \times 211$.

i	$x = x_i$	x_{2i-1}	$y = x_{2i}$	$\lvert y - x \rvert$	$\gcd(y - x, n)$
	2		2		
1	5	5	26	21	1
2	26	677	5524	5498	1
3	677	4821	603	74	37

(3) rho(10277,1,1)=0; algorithm fails since the first time the gcd $\neq 1$ it it is $n = 10277$...

i	$x = x_i$	x_{2i-1}	$y = x_{2i}$	$\lvert y - x \rvert$	$\gcd(y - x, n)$
	1		1		
1	2	2	5	3	1
2	5	26	677	672	1
3	26	6142	7575	7549	1
4	677	4135	7575	6898	1
5	6142	4135	7575	1433	1
6	7575	4135	7575	0	10277

(4) .... so we could try again with a different iteration function (i.e. change c):

rho(10277,2,1)=43, giving factorisation $10277 = 43 \times 239$ ....

i	$x = x_i$	x_{2i-1}	$y = x_{2i}$	$\lvert y - x \rvert$	$\gcd(y - x, n)$
	1		1		
1	3	3	11	8	1
2	11	123	4854	4843	1
3	123	6434	602	479	1
4	4854	2711	1468	3386	1
5	6434	7133	8541	2107	43

(5) .... or we could change the seed,

rho(10277,1,2)=43, giving same factorisation:

i	$x = x_i$	x_{2i-1}	$y = x_{2i}$	$\lvert y - x \rvert$	$\gcd(y - x, n)$
	2		2		
1	5	5	26	21	1
2	26	677	6142	6116	1
3	677	7575	4135	3458	1
4	6142	7575	4135	2007	1
5	7575	7575	4135	3440	43