Pollard Rho factoring algorithm (n, x_1)
Parameter f and X, $x_i \in X$
$x = x_1$
$x' = f(x) \bmod n$
$p = \gcd(x - x', n)$
while $p = 1$
~~$x = x_i$~~
~~$x' = x_{2i}$~~
$x = f(x) \bmod n$
$x' = f(x') \bmod n$
$x' = f(x') \bmod n$
$p = \gcd(x - x', n)$

if $p = n$
return "failure"
else
return p

Example:

$n = 7171 = 71 \times 101$, $f(x) = x^2 + 1$, $x_1 = 1$
then the sequence of x_i's are

1 2 5 26 677 6557 4105

6347 4903 2218 219 4936 4210 4560

4872 375 4377 4389 2016 5471 88

Therefore, if we reduce the values modulo 71

1 2 5 26 38 25 58

28 4 17 6 37 21 16

44 20 46 58 28 4 17

The first collision is

$x_7 \bmod 71 = x_{18} \bmod 71 = 58$

Now, if we apply the algorithm, verify that we would obtain the collision, but for x_{11} and x_{22}.

Dixon's Random Squares Algorithm

Suppose $\exists\, x, y$ s.t $x \not\equiv \pm y \pmod{n}$

but $x^2 \equiv y^2 \bmod n$

$\Rightarrow n \mid (x+y)(x-y)$

but as neither, $x+y$ and $x-y$ are divisible by n, then $\gcd(x+y, n)$ (or $\gcd(x-y, n)$.) is a non trivial factor of n.

Example: Try with $x = 10$, $y = 32$ and

$n = 77$.

~~Random squares algorithm~~

The first step is to choose a factor base, which is a set ~~of~~ B with b smallest prime. Once this set is determined, we first obtain several integers 'z' such that all the prime factors of z^2 mod n occur in the factor base B. Let's see this with an example.

$n = 15770708441$, $b = 6$, $B = \{2, 3, 5, 7, 11, 13\}$

$$8340934156^2 \equiv 3 \times 7 \pmod{n}$$

$$12044942944^2 \equiv 2 \times 7 \times 13 \pmod{n}$$

$$2773700011^2 \equiv 2 \times 3 \times 13 \pmod{n}$$

Note that, ~~all~~ if we compute the product of these 'z's, then every prime in the factor base would be used even number of times.

$$(8340934156 \times 12044942944 \times 2773700011)^2$$

$$\equiv (2 \times 3 \times 7 \times 13)^2 \pmod{n}$$

$$9503435785^2 \equiv 546^2 \pmod{n}$$

Then, we can ~~apply~~ compute

$$\gcd(9503435785 - 546, 1577070841)$$
$$= 115759.$$

which is a factor of n.

<u>In general,</u>

Suppose $B = \{p_1, \ldots, p_b\}$ is the factor base.
Let c be slightly larger than b $(c = b+4)$,
and we want to find 'c' ~~congruencies~~
congruences such that

$$z_j^2 \equiv p_1^{\alpha_{1j}} \times p_2^{\alpha_{2j}} \cdots \times p_b^{\alpha_{bj}} \pmod n, \; 1 \le j \le c$$

Now, we consider the vector

$$a_j = (\alpha_{1j} \bmod 2, \ldots, \alpha_{bj} \bmod 2) \in (\mathbb{Z}_2)^b$$ for
each j

*** If we can find a subset of the a_j's
that sum modulo 2 to the vector $(0, \ldots, 0)$ then
the product of the corresponding z_j's will
use each factor in B an even number of
times.

If we consider the previous ~~exa~~ example.

$a_1 = (0, 1, 0, 1, 0, 0)$

$a_2 = (1, 0, 0, 1, 0, 1)$

$a_3 = (1, 1, 0, 0, 0, 1)$

$a_1 + a_2 + a_3 = (0, 0, 0, 0, 0, 0) \bmod 2$.

~~A~~ Few important points:

(1) Finding a subset of the c vector $a_1, \ldots, a_c$ ~~the~~ that sums modulo 2 to all zero vectors is equivalent to finding a linear dependance ~~of~~ (over $\mathbb{Z}_2$) of these vectors. As we have considered, $c > b$, such linear dependance must exist.

But, generally, c is chosen as ~~[illegible]~~ $> b+1$, so that we can obtain several such congruences ~~such~~ of the form $x^2 \equiv y^2 \pmod{n}$. Hopefully, at least one of the resulting congruences will yield a congruence of the form $x^2 \equiv y^2 \pmod{n}$ where $x \not\equiv \pm y \pmod{n}$

How to find z

We can try to choose the z's in a random manner. But, we can also find z by choosing integers of the form $j + \lceil\sqrt{kn}\rceil$. These integers tend to be small when squared and reduced modulo n, hence have higher probability of factoring over B. We can also try with $z = \lfloor\sqrt{kn}\rfloor$. These integers, when squared and reduced modulo n, are ~~to~~ a bit less than n. This means $-z^2 \bmod n$ is small and can perhaps be easily factored over B. If we include -1 in B, we can factor $z^2 \bmod n$ over B

Example: $n = 1829$, $B = \{-1, 2, 3, 5, 7, 11, 13\}$

$\sqrt{n} = 42.77$, $\sqrt{2n} = 60.48$, $\sqrt{3n} = 74.07$, $\sqrt{4n} = 85.53$

We take $z = 42, 43, 60, 61, 74, 75, 85, 86$.

We can show that

$$z_1^2 \equiv 42^2 \equiv -65 \equiv (-1) \times 5 \times 13$$
$$z_2^2 \equiv 43^2 \equiv 20 \equiv (2^2 \times 5)$$
$$z_3^2 \equiv 61^2 \equiv 63 \equiv (7 \times 3^2)$$
$$z_4^2 \equiv 74^2 \equiv -11 \equiv (-1) \times 11$$
$$z_5^2 \equiv 85^2 \equiv -91 \equiv (-1) \times 7 \times 13$$
$$z_6^2 \equiv 86^2 \equiv 80 \equiv 2^4 \times 5$$

We can find now

$a_1 = (1, 0, 0, 1, 0, 0, 1)$

$a_2 = (0, 0, 0, 1, 0, 0, 0)$

$a_3 = (0, 0, 0, 0, 1, 0, 0)$

$a_4 = (1, 0, 0, 0, 0, 1, 0)$

$a_5 = (1, 0, 0, 0, 1, 0, 1)$

$a_6 = (0, 0, 0, 1, 0, 0, 0)$

We can see that

$a_2 + a_6 = (0, 0, 0, 0, 0, 0, 0) \bmod 2$ — (1)

and

$a_1 + a_2 + a_3 + a_5 = (0, 0, 0, 0, 0, 0, 0) \bmod 2$ — (2)

The first one will not lead to factorization of n

From 2nd equation,

$(42 \times 43 \times 61 \times 85)^2 \equiv (2 \times 3 \times 5 \times 7 \times 13)^2 \bmod 1829$

$\Rightarrow 1459^2 \equiv 901^2 \pmod{1829}$

then $\gcd(1459 + 901, 1829) = 59$ is a factor of n.