Math 259 - Spring 2021
Factorization using difference of squares

Instructions

- The first problem on this assignment is worth 5 points and the second is worth 10 points.
- This assignment is available until Friday May 14 at 11:59pm.
- You can submit a second attempt for this assignment if your first attempt is turned in by Sunday March 21 at 11:59pm.
- If you look up solutions or facts, don't forget to cite your sources and to rephrase everything in your own words.
- You will need to use a calculator or computer for this assignment. You may use addition, multiplication, subtraction, division, the square root function, the modulo operation, and the gcd function. You may also use a function that tells you if an integer is a perfect square.

Problem

1. For each of the following numbers N, compute the values of

$$N + 1^2, N + 2^2, N + 3^2, N + 4^2, \ldots$$

until you find a value $N + b^2$ which is a perfect square: $N + b^2 = a^2$ for a an integer. Then use the values of a and b to factor N. You must state the values of a and b that you found and give the gcd that you computed, as well as give the factors of N.

   (a) $N = 53357$

   (b) $N = 34571$

   (c) $N = 64213$

2. For each of the two values of N below, use the data provided to find values of a and b such that

$$a^2 \equiv b^2 \pmod{N},$$

and use this information to factor N. You must state the values of a and b that you found and give the gcd that you computed, as well as give the factors of N.

   (a) $N = 61063$

$$\begin{aligned} 1882^2 &\equiv 270 \pmod{61063} && \text{and} && 270 = 2 \cdot 3^3 \cdot 5 \\ 1898^2 &\equiv 60750 \pmod{61063} && \text{and} && 60750 = 2 \cdot 3^5 \cdot 5^3 \end{aligned}$$

(b) $N = 2525891$

$$
\begin{array}{lll}
1591^2 \equiv 5390 \pmod{2525891} & \text{and} & 5390 = 2 \cdot 5 \cdot 7^2 \cdot 11 \\
3182^2 \equiv 21560 \pmod{2525891} & \text{and} & 21560 = 2^3 \cdot 5 \cdot 7^2 \cdot 11 \\
4773^2 \equiv 48510 \pmod{2525891} & \text{and} & 48510 = 2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11 \\
5275^2 \equiv 40824 \pmod{2525891} & \text{and} & 40824 = 2^3 \cdot 3^6 \cdot 7 \\
5401^2 \equiv 1386000 \pmod{2525891} & \text{and} & 1386000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11
\end{array}
$$