NT Worksheet-1 Solutions

1) gcd(1160718174, 316258250).

$$1160718174 = 3 \times 316258250 + 211943424$$
$$316258250 = 1 \times 211943424 + 104314826$$
$$211943424 = 2 \times 104314826 + 3313772$$
$$104314926 = 31 \times 3313772 + 1587894$$
$$3313772 = 2 \times 1587894 + 137984$$
$$1587894 = 1 \times 137984 + 70070$$
$$137984 = 1 \times 70070 + 67914$$
$$70070 = 1 \times 67914 + 2156$$
$$67914 = 31 \times 2156 + 1078$$
$$2156 = 2 \times 1078 + 0$$

Hence 1078 is the gcd.

2) Let $b = r_0, r_1, r_2, \ldots$ be the successive remainders in the Euclidean algorithm applied to a and b. Show that after every 2 steps, the remainder is reduced by atleast one half. In other words, verify that

$$r_{i+2} < \frac{1}{2} r_i \qquad \forall\, i = 0, 1, 2, \ldots$$

If $b = r_0, r_1, r_2, \ldots$ be the successive remainders in the Euclidean Algorithm, then,

$$a = r_0 q_0 + r_1, \text{ where } r_0 > r_1 \geq 0 \text{ and } q_0 \geq 1$$
$$r_0 = r_1 q_1 + r_2, \text{ where } r_1 > r_2 \geq 0 \text{ and } q_1 \geq 1$$
$$r_1 = r_2 q_2 + r_3, \text{ where } r_2 > r_3 \geq 0 \text{ and } q_2 \geq 1$$
$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

So, we can see $\forall\, i = 0, 1, 2, \ldots$

$$r_i = r_{i+1} q_{i+1} + r_{i+2} \quad \text{where } r_{i+1} > r_{i+2} \geq 0 \text{ and } q_{i+1} \geq 1$$

Now since $r_{i+1} > r_{i+2}$ and $q_{i+1} \geq 1$,

$$r_{i+1} q_{i+1} > r_{i+2}$$

$$\Rightarrow \quad r_{i+2} + r_{i+1} q_{i+1} > r_{i+2} + r_{i+2}$$

$$\Rightarrow \quad r_i > 2 r_{i+2}$$

$$\Rightarrow \quad r_{i+2} < \frac{r_i}{2} \qquad \forall i = 1, 2, 3, \ldots$$

3) It is believed that there are infinitely many primes of the form $N^2 + 1$, but no one knows for sure.

a) Do you think there are infinitely many primes of the form $N^2 - 1$?
b) Do you think there are infinitely many primes of the form $N^2 - 2$?
c) How about $N^2 - 3$? $N^2 - 4$?
d) Which values of a do you think give infinitely many primes of the form $N^2 - a$?

a) Note that, $N^2 - 1 = (N-1)(N+1)$

Here both the factors are > 1 unless, $N = 2$, for which $N^2 - 1$ is 3 which is a prime. 3 is the only prime of the form $N^2 - 1$. Hence there are not infinitely many primes of the form $N^2 - 1$.

For part b, c, d any reasonable attempt which leads you to conjecture that "there are infinitely many primes of the form $N^2 - a$ if a is not a perfect square" would receive full credit.

For $N^2 - 4$, we expect you to have shown the factorization $N^2 - 4 = (N+2)(N-2)$ and similar reasoning as in part (a).