HOMEWORK

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (3.24) For each of the following numbers N, compute the values of
$$N + 1^2, N + 2^2, N + 3^2, N + 4^2, \ldots$$
as we did in Example 3.34 until you find a value $N + b^2$ that is a perfect square a^2. Then the use the values of a and b to factor N.
   (a) $N = 53357$
   (b) $N = 34571$
   (c) $N = 25777$
   (d) $N = 64213$

(2) (3.26) For each part, use the data provided to find the values of a and b satisfying $a^2 = b^2 \mod n$, and then compute $\gcd(N, a - b)$ in order to find a nontrivial factor of N, as we did in Examples 3.37 and 3.38.
   (a) $N = 61063$
$$\begin{aligned} 1882^2 &= 270 \mod 61063 \text{ and } 270 &&= 2 \cdot 3^3 \cdot 5 \\ 1898^2 &= 60750 \mod 61063 \text{ and } 60750 &&= 2 \cdot 3^5 \cdot 5^3 \end{aligned}$$
   (b) $N = 52907$
$$\begin{aligned} 399^2 &= 480 \mod 52907 \text{ and } 480 &&= 2^5 \cdot 3 \cdot 5 \\ 763^2 &= 192 \mod 52907 \text{ and } 192 &&= 2^6 \cdot 3 \\ 773^2 &= 15552 \mod 52907 \text{ and } 15552 &&= 2^6 \cdot 3^5 \\ 976^2 &= 250 \mod 52907 \text{ and } 250 &&= 2 \cdot 5^3 \end{aligned}$$
   (c) $N = 198103$
$$\begin{aligned} 1189^2 &= 27000 \mod 198103 \text{ and } 27000 &&= 2^3 \cdot 3^3 \cdot 5^3 \\ 1605^2 &= 686 \mod 198103 \text{ and } 686 &&= 2 \cdot 7 \\ 2378^2 &= 108000 \mod 198103 \text{ and } 108000 &&= 2^5 \cdot 3^3 \cdot 5^3 \\ 2815^2 &= 105 \mod 198103 \text{ and } 105 &&= 3 \cdot 5 \cdot 7 \end{aligned}$$
   (d) $N = 2525891$
$$\begin{aligned} 1591^2 &= 5390 \mod 2525891 \text{ and } 5390 &&= 2 \cdot 5 \cdot 7^2 \cdot 11 \\ 3182^2 &= 21560 \mod 2525891 \text{ and } 21560 &&= 2^3 \cdot 5 \cdot 7^2 \cdot 11 \\ 4773^2 &= 108000 \mod 2525891 \text{ and } 108000 &&= 2^5 \cdot 3^3 \cdot 5^3 \\ 2815^2 &= 105 \mod 2525891 \text{ and } 105 &&= 3 \cdot 5 \cdot 7 \end{aligned}$$

(a) $N = 61063$

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

(b) $N = 52907$

$$\begin{aligned} 399^2 &= 480 \mod 52907 \quad \text{and} \quad 480 &&= 2^5 \cdot 3 \cdot 5 \\ 763^2 &= 192 \mod 52907 \quad \text{and} \quad 192 &&= 2^6 \cdot 3 \\ 773^2 &= 15552 \mod 52907 \quad \text{and} \quad 15552 &&= 2^6 \cdot 3^5 \\ 976^2 &= 250 \mod 52907 \quad \text{and} \quad 250 &&= 2 \cdot 5^3 \end{aligned}$$

(c) $N = 198103$

$$\begin{aligned} 1189^2 &= 27000 \mod 198103 \quad \text{and} \quad 27000 &&= 2^3 \cdot 3^3 \cdot 5^3 \\ 1605^2 &= 686 \mod 198103 \quad \text{and} \quad 686 &&= 2 \cdot 7^3 \\ 2378^2 &= 108000 \mod 198103 \quad \text{and} \quad 108000 &&= 2^5 \cdot 3^3 \cdot 5^3 \\ 2815^2 &= 105 \mod 198103 \quad \text{and} \quad 105 &&= 3 \cdot 5 \cdot 7 \end{aligned}$$

(d) $N = 2525891$

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

(3) (3.27) Compute the followimg values of $\psi(X, B)$, the number of B-smooth numbers between 2 and X (see page 150).
  (a) $\psi(25, 3)$
  (b) $\psi(35, 5)$
  (c) $\psi(50, 7)$
  (d) $\psi(100, 5)$
  (e) $\psi(100, 7)$
(4) (3.34) Illustrate the quadratic sieve, as was down in Fig. 3.3 (page 161), by sieving prime powers up to B on the values of $F(T) = T^2 - N$ in the indicated range.
  (a) Sieve $N = 493$ using prime powers up to $B = 11$ on values from $F(23)$ to $F(38)$. Use the relation(s) that you find to factor N.
  (b) Extend the computation in (a) by using prime powers up to $B = 16$ and sieving values from $F(23)$ to $F(50)$. What additional value(s) are sieved down to 1 and what additional relation(n) do they yield?
(5) (3.35) Let $\mathbb{Z}[\beta]$ be the ring described in Example 3.55, i.e. β is a root of $f(x) = 1 + 3x - 2x^3 + x^4$. For each of the following pairs of elements $u, v \in \mathbb{Z}[\beta]$, compute the sum $u + v$ and the product uv. Your answers should only involve powers of β up to β^3.

(a) $u = -5 - 2\beta + 9\beta^2 - 9\beta^3$ and $v = 2 + 9\beta - 7\beta + 7\beta^2$.
(b) $u = 9 + 9\beta + 6\beta^2 - 5\beta^3$ and $v = -4 - 6\beta - 2\beta^2 - 5\beta^3$.
(c) $u = 6 - 5\beta + 3\beta^2 + 3\beta^3$ and $v = -2 + 7\beta + 6\beta^2$.