Section 3.5 Page 143

$n = a^2 - b^2 = (a-b)(a+b)$

Factorize $n = 391$.

$\sqrt{391} = 19.77$ (2 dp)

$\lceil \sqrt{391} \rceil = 20 = a$

$391 = 20^2 - b^2 \Rightarrow b^2 = 20^2 - 391 = 9 = 3^2$

Therefore $n = a^2 - b^2$

$391 = 20^2 - 3^2$

$= (20-3)(20+3)$

$= 17 \times 23$

Example 3.26 on Page 144

Factorize 13 081

Soln:

$n = a^2 - b^2 = (a-b)(a+b)$

$n = 13\,081$

$a = \lceil \sqrt{13\,081} \rceil = \lceil 114.37 \rceil = 115$

$13\,081 = 115^2 - b^2$

$b^2 = 115^2 - 13\,081 = 144 = 12^2$

$13\,081 = 115^2 - 12^2$

$= (115-12)(115+12)$

$= 103 \times 127.$

We need to check whether 103 and 127 are prime.

(2.10) $p \leq \lfloor \sqrt{m} \rfloor$

$p \leq \lfloor \sqrt{103} \rfloor = 10$

Test primes 2, 3, 5, 7 as factors of 103. None of these are factors of 103 so 103 is prime. Similarly 127 is prime.

Hence $13\,081 = 103 \times 127$.

3.5.3 Fermat Factorization Page 144

Example 3.27 Page 145

Factorize 12 371 into prime factors.

Soln:

$$n = 12\,371 = a^2 - b^2$$

$$a_1 = \lceil \sqrt{12\,371} \rceil = 112$$

We have $b_1^2 = a_1^2 - n = 112^2 - 12\,371 = 173$. ×

173 is not a square

$$113^2 - 12\,371 = 398 \times$$

$$114^2 - 12\,371 = 625 = 25^2$$

$$12\,371 = 114^2 - 25^2$$

$$= (114 - 25)(114 + 25)$$

$$= 89 \times 139$$

Both 89 and 139 are prime.

$$12\,371 = 89 \times 139.$$

3.5.4 Factorization using Modular arithmetic. Page 146.

Fac Theorem (3.26)

$a^2 \equiv b^2 \pmod n$ $\quad a \not\equiv \pm b \pmod n$

then $\gcd(a-b, n)$ is a non-trivial factor of n.

Proof.

Let $g = \gcd(a-b, n)$.

By defn of gcd $g \mid n$. We need to show $g \neq 1$ and $g \neq n$.

Case I $g \neq n$.

we have $a^2 \equiv b^2 \pmod n$ but $a \not\equiv b \pmod n \Rightarrow n \nmid (a-b)$

$g = \gcd(a-b, n) \neq n$.

Case II $g \neq 1$.

$a^2 \equiv b^2 \pmod n \iff a^2 - b^2 \equiv (a-b)(a+b) \equiv 0 \pmod n$

By defn of congruence

$(a-b)(a+b) \equiv 0 \pmod n \Rightarrow n \mid (a-b)(a+b)$

$a \not\equiv -b \pmod n$

$\Rightarrow a+b \not\equiv 0 \pmod n$

$\Rightarrow n \nmid (a+b)$

By Supplementary Problem question 1.22

If $x \nmid y$ but $x \mid yz$ then $\gcd(x, z) > 1$

$n \mid (a-b)(a+b)$ $\quad n \nmid (a+b) \Rightarrow g = \gcd(n, a-b) > 1$