Do the following exercises from the text:
Section 6.3: 1, 2, 3, 4

1. Suppose that A is a member of an RSA public-key system and that his choices for r and s are $r = 53 \cdot 71 = 3763$ and $s = 11$. If B wants to send the message NOW to A, what is actually transmitted.

▶ **Solution.** Since $r = 3763$ the largest block that can be represented is 2 letters. So break NOW into blocks of 2 letters by appending a letter, say X, to the end, to get two blocks NO, represented as 1314, and WX, represented as 2223. What is transmitted is $1314^{11} \equiv 1265 \pmod{3763}$ for NO, and $2223^{11} \equiv 3583 \pmod{3763}$ for WX. ◀

2. Suppose that A is as in Exercise 1 and A received from B the ciphertext message 0737 1627.

(a) Compute A's deciphering key.

▶ **Solution.** The deciphering key t is the solution to $st \equiv 1 \pmod{\phi(r)}$. Since $\phi(r) = (53-1)(71-1) = 3640$, t is the solution to $11t \equiv 1 \pmod{3640}$. Applying the Euclidean Algorithm to find the greatest common divisor of 11 and 3640 gives $t = 331$. ◀

(b) Decipher B's message to A.

▶ **Solution.** To decipher, compute $737^{331} \equiv 18 \pmod{3763}$ which corresponds to 0018 or AS, and compute the second block as $1627^{331} \equiv 1524 \pmod{3763}$ which corresponds to PY. Thus, the deciphered message is $A\ SPY$. ◀

3. Let $r = pq$, where p and q are primes with $p > q$.

(a) Show that $p + q = r - \phi(r) + 1$.

▶ **Solution.** $\phi(r) = (p-1)(q-1) = pq - p - q + 1$,so $p + q = r - \phi(r) + 1$. ◀

(b) Show that $p - q = \sqrt{(p+q)^2 - 4r}$.

▶ **Solution.** $\sqrt{(p+q)^2 - 4r} = \sqrt{p^2 + 2pq + q^2 - 4pq} = \sqrt{(p-q)^2} = p - q$ since $p > q$. ◀

(c) Find p and q in terms of $\phi(r)$ and r.

▶ **Solution.** Since $p = ((p+q)+(p-q))/2$, using the formulas from (a) and (b) gives

$$\begin{aligned} p &= \frac{r - \phi(r) + 1 + \sqrt{(p+q)^2 - 4r}}{2} \\ &= \frac{r - \phi(r) + 1 + \sqrt{(r - \phi(r) + 1)^2 - 4r}}{2}. \end{aligned}$$

Similarly, since $q = ((p+q) - (p-q))/2$, we have

$$\begin{aligned} q &= \frac{r - \phi(r) + 1 - \sqrt{(p+q)^2 - 4r}}{2} \\ &= \frac{r - \phi(r) + 1 - \sqrt{(r - \phi(r) + 1)^2 - 4r}}{2}. \end{aligned}$$

◀

4. If $r = 1829$ and $\phi(r) = 1740$ use the results of Exercise 3 to determine p and q.

▶ **Solution.**

$$\begin{aligned} p &= \frac{1829 - 1740 + 1 + \sqrt{(1829 - 1740) + 1)^2 - 4 \cdot 1829}}{2} \\ &= \frac{90 + \sqrt{90^2 - 7316}}{2} \\ &= \frac{90 + 28}{2} = 59. \end{aligned}$$

Similarly,

$$\begin{aligned} p &= \frac{1829 - 1740 + 1 - \sqrt{(1829 - 1740) + 1)^2 - 4 \cdot 1829}}{2} \\ &= \frac{90 - \sqrt{90^2 - 7316}}{2} \\ &= \frac{90 - 28}{2} = 31. \end{aligned}$$

◀

Section 2.6: 1, 3, 9, 10

1. Construct a table of primitive Pythagorean triples for the following values of (s, t): (1, 2), (1, 4), (2, 3), (1, 6), (2, 5), (3, 4), (1, 8), (2, 7) and (4, 5).

▶ **Solution.**

s	1	1	2	1	2	3	1	2	4
t	2	4	3	6	5	4	8	7	5
x	4	8	12	12	20	24	16	28	40
y	3	15	5	35	21	7	63	45	9
z	5	17	13	37	29	25	65	53	41

◀

3. Give values of x, y, z such that $(x, y, z) = 1$ and yet $(x, y) > 1$, $(x, z) > 1$, and $(y, z) > 1$.

▶ **Solution.** $x = 2 \cdot 3$, $y = 3 \cdot 5$, and $z = 2 \cdot 5$ will do. ◀

9. Show that the only Pythagorean triples in arithmetic progression are of the form $(3k, 4k, 5k)$ for $k \geq 1$.

▶ **Solution.** Without loss of generality, we may suppose that a, $a + k$, $a + 2k$ with $a > 0$, $k > 0$ form a Pythagorean triple. Then $a^2 + (a + k)^2 = (a + 2k)^2$, so that

$$a^2 + a^2 + 2ak + k^2 = a^2 + 4ak + 4k^2.$$

Hence, $a^2 - 2ak - 3k^2 = 0$ so that $(a + k)(a - 3k) = 0$ and $a = 3k$ since $a = -k$ is not possible since $k > 0$ and $a > 0$. Then $a = 3k$, $a + k = 4k$, and $a + 2k = 5k$ as claimed. ◀

10. Show that any positive odd integer can be the side of a primitive Pythagorean triangle whose other side and hypotenuse are consecutive integers.

▶ **Solution.** Let $y = 2k + 1$ be any positive integer, let $x = a$ and $z = a + 1$. Since $(a, a+1) - 1$, it is clear that $(a, 2k+1, a+1) = 1$ also. Now, x, y, z form a Pythagorean triple if and only if $a^2 + (2k + 1)^2 = (a + 1)^2$. Solving for a gives $a = 2k^2 + 2k$. Thus, the desired triple is $x = 2k^2 + 2k$, $y = 2k + 1$, $z = 2k^2 + 2k + 1$. ◀