Exercises for practice: Do the following exercises from the text:

Section NT-1 (page 60): 1.1, 1.2, 1.3, 1.4, 1.6, 1.7, 1.13, 1.14, 1.15, 1.17.
Section NT-2 (page 76): 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8.

These exercises have (as do all the exercises from the text) solutions in the Solutions section.

Exercises to turn in from the number theory handout:
From Pages 9–10:

1. By using the Euclidean algorithm find the greatest common divisor (g.c.d.) of

   (a) 7469 and 2464;

   ▶ **Solution.** Using the division algorithm repeatedly gives:

   $$\begin{aligned} 7469 &= 2464 \cdot 3 + 77 \\ 2464 &= 77 \cdot 32 + 0. \end{aligned}$$

   Hence the greatest common divisor is (7469, 2464) = 77. ◀

   (c) 2947 and 3997;

   ▶ **Solution.** Using the division algorithm repeatedly gives:

   $$\begin{aligned} 3997 &= 1 \cdot 2947 + 1050 \\ 2947 &= 2 \cdot 1050 + 847 \\ 1050 &= 1 \cdot 847 + 203 \\ 847 &= 4 \cdot 203 + 35 \\ 203 &= 5 \cdot 35 + 28 \\ 35 &= 1 \cdot 28 + 7 \\ 28 &= 4 \cdot 7 + 0. \end{aligned}$$

   Hence the greatest common divisor is (3997, 2947) = 7. ◀

2. Find the greatest common divisor g of the numbers 1819 and 3587, and then find integers x and y to satisfy $1819x + 3587y = g$.

   ▶ **Solution.** Use the Euclidean algorithm to find g:

   $$\begin{aligned} 3587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \\ 1768 &= 51 \cdot 34 + 34 \\ 51 &= 34 \cdot 1 + 17 \\ 34 &= 17 \cdot 2 + 0. \end{aligned}$$

Hence the greatest common divisor is $g = (3587, 1819) = 17$. To find x and y reverse the chain of equalities used in the Euclidean algorithm:

$$\begin{aligned} 17 &= 51 - 34 \cdot 1 \\ &= 51 - (1768 - 51 \cdot 34) \\ &= 51 \cdot 35 - 1768 \\ &= (1819 - 1768) \cdot 35 - 1768 \\ &= 1819 \cdot 35 - 1768 \cdot 36 \\ &= 1819 \cdot 35 - (3587 - 1819) \cdot 36 \\ &= 1819 \cdot 71 - 3587 \cdot 36. \end{aligned}$$

Thus, we have written $g = 17 = 1819 \cdot 71 - 3587 \cdot 36 = 1819x + 3587y$, where $x = 71$ and $y = -36$. ◀

3. Find values of x and y to satisfy

   (a) $243x + 198y = 9$;

   ▶ **Solution.** Start by find the greatest common divisor of 243 and 198 via the Euclidean algorithm:

$$\begin{aligned} 243 &= 198 \cdot 1 + 45 \\ 198 &= 45 \cdot 4 + 18 \\ 45 &= 18 \cdot 2 + 9. \end{aligned}$$

   Since 9 divides 18, it follows that 9 is the greatest common divisor of 243 and 198. Now reverse the steps to write 9 as a combination of 243 and 198:

$$\begin{aligned} 9 &= 45 - 18 \cdot 2 \\ &= 45 - (198 - 45 \cdot 4) \cdot 2 \\ &= 45 \cdot 9 - 198 \cdot 2 \\ &= (243 - 198) \cdot 9 - 198 \cdot 2 \\ &= 243 \cdot 9 - 198 \cdot 11. \end{aligned}$$

   Hence $9 = 243x + 198y$ where $x = 9$ and $y = -11$. ◀

   (c) $43x + 64y = 1$.

   ▶ **Solution.** Use the Euclidean algorithm:

$$\begin{aligned} 64 &= 43 + 21 \\ 43 &= 21 \cdot 2 + 1. \end{aligned}$$

Thus

$$\begin{aligned} 1 &= 43 - 21 \cdot 2 \\ &= 43 - (64 - 43) \cdot 2 \\ &= 43 \cdot 3 - 64 \cdot 2. \end{aligned}$$

Hence, if $x = 3$ and $y = -2$, we have $1 = 43x + 64y$. ◀

10. Given $a|b$ and $c|d$ prove that $ac|bd$.

    Proof. Assuming that $a|b$ and $c|d$ means that we can write $b = ax$ and $d = cy$ where x and y are integers. Then $bd = (ax)(cy) = (ac)(xy)$. Since xy is an integer (because the product of integers is an integer) we have that $bd = (ac)w$ where w is an integer. This is what is means for ac to divide bd. □

12. Given that $(a,\, 4) = 2$ and $(b,\, 4) = 2$, prove that $(a + b,\, 4) = 4$.

    Proof. Since the positive divisors of 4 are 1, 2, and 4, the fact that $(a,\, 4) = 2$ means that $2|a$, but 4 does not divide a. Hence we can write $a = 2k$ where k is not divisible by 2, that is k is odd so that $a = 2(2m + 1)$. Similarly, the fact that $(b,\, 4) = 2$ means that $b = 2(2n+1)$. Then, $a+b = 2(2m+1)+2(2n+1) = 2(2m+2n+2) = 4(m+n+1)$ so that $4|(a + b)$ and hence $(a + b,\, 4) = 4$ since there cannot be a divisor of 4 larger than 4. □

21. Prove that if an integer is of the form $6k + 5$ then it is necessarily of the form $3k - 1$, but not conversely.

    Proof. Let n be an integer of the form $6k+5$. This means that we can write $n = 6k+5$ for some choice of the integer k. Since $6 = 5 - 1$, we can then write $n = 6k + 5 = 6k + 6 - 1 = 6(k + 1) - 1 = 3(2(k + 1)) - 1 = 3r - 1$. That is, if $n = 6k + 5$, then we can also write n as 3 times an integer (namely $2(k + 1)$) minus 1, which is what is required for n to have the form $3k + 1$. (Note that the *same* k is not used in both representations.)

    The converse statement is not true, since 2 is an integer that can be written in the form $3k - 1$ (using $k = 1$), but 2 cannot be written in the form $6k + 5$ for any choice of k since if $6k + 5 = 2$ this requires that $6k = -3$ for some integer k. But $k = -1/2$ is not an integer. □

From Page 18:

16. If $(a,\, b) = p$, a prime, what are the possible values of $(a^2,\, b)$? of $(a^3,\, b)$? of $(a^2,\, b^3)$?

► **Solution.** Since $(a, b) = p$ we can write $a = pr$ and $b = ps$ where r and s are integers such that $(r, s) = 1$. Then $a^2 = p^2r^2$. Then by Theorem 1.7, $(a^2, b) = (p^2r^2, ps) = p(pr^2, s)$. By Theorem 1.8, $(r^2, s) = 1$. Thus, there are two cases to consider: if $p|s$ then $(a^2, b) = p^2$, and if $p \nmid s$ then $(pr^2, s) = 1$ (again by Theorem 1.8) so that $(a^2, b) = p$ in that case. Thus, there are two cases for (a^2, b): namely p or p^2. The same analysis shows that (a^3, b) must be either p, p^2, or p^3, depending on the power of p that divides b. Analyze (a^2, b^3) as follows. Using the notation already introduced, and Theorem 1.7, we get $(a^2, b^3) = (p^2r^2, p^3s^3) = p^2(r^2, ps^3)$. Since $(r, s) = 1$, Theorem 1.8 shows that $(r^2, s^3) = 1$. Thus, there are two possibilities for (a^2, b^3):

$$\begin{cases} (a^2, b^3) = p^2 & \text{if } p \nmid r, \\ (a^2, b^3) = p^3 & \text{if } p|r. \end{cases}$$

◄

18. If a and b are represented by (1.6), what conditions must be satisfied by the exponents is a is to be a perfect square? A perfect cube? For $a|b$? For $a^2|b^2$?

► **Solution.** Using the notation of equation (1.6), a is a perfect square if each of the exponents α_j is even, a is a perfect cube if each of the exponents α_j is a multiple of 3, $a|b$ if and only if $\alpha_j \le \beta_j$ for each j, and the same condition is necessary for a^2 to divide b^2. ◄

24. Determine whether the following statements are true or false. If true, prove the result, and if false, give a counterexample.

(1) If $(a, b) = (a, c)$, then $[a, b] = [a, c]$.

► **Solution. False.** Counterexample: $a = 2$, $b = 3$, $c = 5$. Then $(a, b) = (a, c) = 1$ but $[a, b] = 6 \ne 10 = [a, c]$. ◄

(2) If $(a, b) = (a, c)$ then $(a^2, b^2) = (a^2, c^2)$.

► **Solution. True.**

Proof. Suppose first that r and s are integers such that $(r, s) = 1$. Then by Theorem 1.8 (Page 6) (letting $a = r$, $b = r$ and $m = s$) it follows that $(r^2, s) = 1$ and applying this result a second time (with $a = b = s$, $m = r^2$) gives $(r^2, s^2) = 1$, so that $(r, s) = (r^2, s^2)$ if $(r, s) = 1$.
Now suppose that $(a, b) = d$ and let $r = a/d$, $s = b/d$. Then by Theorem 1.7 (Page 6) we get that $(r, s) = (a, b)/d = 1$ so that we can apply the previous paragraph (and Theorem 1.6) to get

$$(a^2, b^2) = (d^2r^2, d^2s^2) = d^2(r^2, s^2) = d^2 = (a, b)^2.$$

Assuming that $(a, b) = (a, c)$ we get

$$(a^2, b^2) = (a, b)^2 = (a, c)^2 = (a^2, c^2).$$

□

This can also be proved using the factorization into primes given by formula (1.6) (Page 15). ◀

(3) If $(a, b) = (a, c)$ then $(a, b) = (a, b, c)$.

▶ **Solution. True.**

Proof. Suppose $d = (a, b)$. Then $d|a$, $d|b$, and since we are assuming that $d = (a, b) = (a, c)$ it follows that $d|c$. Thus d is a common divisor of a, b, and c so $d \le (a, b, c)$. But if e is any common divisor of a, b, and c, then certainly e is a common divisor of a and b so that $e \le d = (a, b)$. Hence, if we take e to be the common divisor (a, b, c) we have that $(a, b, c) \le d$. Hence, $(a, b) = d = (a, b, c)$. □

◀

(4) If p is a prime and $p|a$ and $p|(a^2 + b^2)$ then $p|b$.

▶ **Solution. True.** If $p|a$ then $p|a^2$. If p also divides $a^2 + b^2$ then p divides $(a^2 + b^2) - a^2 = b^2$. By Theorem 1.15, if $p|b^2$ then $p|b$. ◀

(5) If p is a prime and $p|a^7$, then $p|a$.

▶ **Solution. True.** This follows directly from Theorem 1.15. ◀

(6) If $a^3|c^3$, then $a|c$.

▶ **Solution.** Writing a and c in the form of formula (1.6) gives

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad \text{and} \quad c = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},$$

so that

$$a^3 = p_1^{3\alpha_1} p_2^{3\alpha_2} \cdots p_r^{3\alpha_r}, \quad \text{and} \quad c^3 = p_1^{3\beta_1} p_2^{3\beta_2} \cdots p_r^{3\beta_r}.$$

Thus $a^3|c^3$ if and only if $3\alpha_j \le 3\beta_j$ for $j = 1, 2, \ldots, r$, and this is true if and only if $\alpha_j \le \beta_j$ for $j = 1, 2, \ldots, r$, which is true if and only if $a|c$. ◀

(7) if $a^3|c^2$ then $a|c$.

▶ **Solution. True.** In the notation of part (6), $a^3|c^2$ if and only if $3\alpha_j \le 2\beta_j$ for all j, and this is true if and only if $\alpha_j \le (2/3)\beta_j < \beta_j$. But this is precisely the condition that guarantees that $a|c$. ◀

(8) If $a^2|c^3$, then $a|c$.

▶ **Solution. False.** A counterexample is $a = 8$, $c = 4$. Then $a^2 = 64 = c^3$ but $8 \nmid 4$. ◀