MATH 115: ERRATA IN *ELEMENTARY NUMBER THEORY*, FOURTH EDITION BY KENNETH H. ROSEN

Compiled by Ken Ribet and members of his 115 class (taught in Spring 2001) (Lizet Mendoza, Grace Wang, Noah Zaitlen) and John Voight and his 115 class (taught in Summer 2004) (Jeff Brown, Cliff Cheng, Chris Crutchfield, Aaron Dall, James Godzik, Nancy Lin, Alex Shlafer, David Turner). Contribute your own errata to `jvoight@math.berkeley.edu`.

(1) p. 32, Proof of Theorem 1.7: "T has a least element $k = q$" should read "T has a least element $r = a - bq$".
(2) p. 35, Exercise 1.4.18: The problem is incorrect. Either you should restrict to $0 \leq r \leq b/2$ (but then you have to worry about endpoints), or you should have no reference to e, and the problem should be: $a = bq + r$ with $-b/2 < r \leq b/2$.
(3) p. 49: The usual word size for Pentium machines is 2^{32}, not 2^{35}. (Also figured elsewhere in the text, e.g. p. 147.)
(4) p. 68, sieve of Eratosthenes: The prime 2 is crossed out, and the nonprime 1 is not crossed out.
(5) p. 77, Exercise 10: It appears that you need Lemma 3.5 (§3.4) to prove this, since you need to know if $p \mid q_1 q_2 \dots q_m$ then $p \mid q_i$ for some i (so $p = q_i$).
(6) p. 83, Example 3.11: Toward the end, you write 32 instead of 35.
(7) p. 92, Theorem 3.13: Not true that $\gcd(a, b) = s_0 a + t_0 b$ since $s_0 = 1$ and $t_0 = 0$. The statement may be true when n is equal to the number of divisions in Euclidean algorithm, but it is not true for $n = 0, 1, \dots$.
(8) p. 97, Lemma 3.4: Refers to Theorem 1.5, which should be Theorem 1.6.
(9) p. 97, Lemma 3.5: In the proof, explain how Lemma 3.4 implies $p \mid a_{n+1}$ or $p \mid (a_1 \dots a_n)$.
(10) p. 101, Theorem 7.8: In the proof, Lemma 3.6 should be Lemma 3.7.
(11) p. 103, Example 3.20: Refers to Exercise 32 (which is irrelevant to the problem) and Exercise 40 (which is trivial, you should instead refer to Lemma 3.5).
(12) p. 107, Exercise 3.4.47: Define "not a power of p".
(13) p. 109, Exercise 3.4.77: Concerning the solution in the back, p. 569, "Exercise 65" should be Exercise 75.
(14) p. 121, Theorem 3.21: In the proof (halfway down the page), Theorem 3.7 should be Theorem 3.6.
(15) p. 131, before Corollary 4.4.1: Grammar error: "cancel number*s*."
(16) p. 131, Theorem 4.5: This follows immediately from Theorem 4.3, and should either be a remark or a corollary. (E.g. $a + c \equiv b + c \equiv d + c = c + d \pmod{m}$.)
(17) p. 136, Exercise 4.20: Need n divisible by 4 *and positive*.

Date: July 27, 2004.

(18) p. 142, Exercise 4.2.4: Is the problem asking:

$$m = a\lfloor m/a \rfloor + a_1$$
$$m = a_1\lfloor m/a_1 \rfloor + a_2$$
$$\vdots$$

where $0 < 1 = a_n < a_{n-1} < \cdots < a_2 < a_1 < a$?

This algorithm fails. Take $a = 5$, $m = 12$, $b = 1$ and solve

$$5x \equiv 1 \pmod{12}.$$

Then $a_1 = (m \bmod a) = 2$ and $\lfloor m/a \rfloor = 2$ so we obtain

$$2x \equiv -2 \pmod{12}.$$

Already $x = -1$ is not a solution to the original congruence. If we continue, we obtain $a_2 = (m \bmod a_1) = 0$, which disproves part (b). Perhaps the algorithm works only when m is prime?

Or is this the Euclidean algorithm?

$$m = \lfloor m/a \rfloor a + a_1$$
$$a = \lfloor a/a1 \rfloor a_1 + a_2$$
$$a_1 = \lfloor a_1/a_2 \rfloor + a_3$$
$$\vdots$$

(19) p. 142, Exercises 4.2.10–11: In parts (b), “module” should be ”modulo”.

(20) p. 150, Exercise 4.3.14: One solution is to apply Exercise 15 (which follows) to $x \equiv b \pmod{a}$ and $x \equiv b \pmod{c}$. So put this exercise afterwards.

(21) p. 150, Exercise 4.3.15: This concerns the solution in the back, p. 574. At the end, you cannot apply the CRT as stated in the text because $\gcd(m_1/\gcd(m_1, m_2), m_2)$ may not be equal to 1 (e.g. $m_1 = 12$, $m_2 = 18$).

Instead: There is a solution $x \in \mathbb{Z}$ to the congruences if and only if there is a solution $k \in \mathbb{Z}$ to

$$x = a_1 + km_1 \equiv a_2 \pmod{m_2}$$

i.e.

$$a_1 - a_2 \equiv -km_1 \pmod{m_2}.$$

By §4.2, this has a solution if and only if $\gcd(m_1, m_2) \mid (a_1 - a_2)$. To show uniqueness, suppose $x, x' \in \mathbb{Z}$ are solutions, then

$$x \equiv x' \equiv a_i \pmod{m_i}$$

so $m_i \mid (x - x')$ and by a previous exercise $\operatorname{lcm}(m_1, m_2) \mid (x - x')$.

(22) p. 158, Example 4.23: The $f'(2)$ in computing r_3 should be $\overline{f'(2)}$.

(23) p. 158, Exercise 4.3.1(c): Should be $4x$ not $4x^2$ to match (a) and (b). Also, the $=$ signs should be $\equiv$.

(24) p. 197: Near the bottom, “the fact that p divides $(p + 1)! + 1$” should be $(p - 1)!$.

(25) p. 203, Exercise 6.1.33: Regarding the solution in the back, p. 579, towards the middle it should read $(p - 1)! \equiv -1$, not $p!$.

(26) p. 213, Exercise 6.2.6: The hint should read $a^{2p} \equiv 1 \pmod{n}$.

(27) p. 225, Theorem 7.6: In the middle of the proof, $a_j \geq 1$ should be $a_j > 1$.

(28) p. 229, Exercise 7.1.26: The statement is false for $n = 2$.
(29) p. 230: In the biography of Liouville, near the bottom it should be, "He is also know$n$ today".
(30) p. 248, Exercise 7.3.3: In the solution in the back, for (b) and (c) you list the numbers themselves! This makes it seem like these numbers are prime, or at least that the problem is trivial. Better to list factors $2^d - 1$, for $d \mid 91, 1001$, respectively.
(31) p. 253, Theorem 7.15: In the last line of the page, $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a^t}$. Should be subscripted, not superscripted.
(32) p. 256, Exercise 7.4.17: You may have the multiplicative function $f(n) = 0$ for all n, so either you should insist that $f(1) = 1$, or change the formula to read

$$\sum_{d|n} \mu(d) f(d) = (f(1) - f(p_1)) \cdots (f(1) - f(p_k)).$$

(33) p. 257, Exercise 7.4.21: The answer in the back should be

$$(-1)^k \prod_{i=1}^{k} p_i.$$

(34) p. 267, Exercise 8.1.12: Ciphertext should start `LFDPH`.
(35) Section 8.3: For exponentiation ciphers and RSA, students will ask what happens if P is not invertible modulo p (or modulo n). If the plaintext is `AAAAA...A`, then the integer value of P is just 0. (Perhaps just reference the exercise 8.4.3?)
(36) p. 287: Should have $E(P) = C \equiv P^e \pmod{n}$, not $\pmod{p}$. In the next indented equation, the capital P erroneously is listed as lowercase p.
(37) Section 8.5: You should explain what knapsack problems have to do with knapsacks. The first example presented, Example 8.16, doesn't seem to be an example of what is described in the paragraph above it because there is no S in the picture.
(38) p. 307: At the bottom, you should have $x^U \equiv 1 \pmod{n}$, not $= 1$, and it is not for all integers x, but only those for which $\gcd(x, n) = 1$.
(39) p. 308–309: Why do you switch the modulus between m and n?
(40) p. 308, Theorem 9.1: The first formatted equation has many typos, it should read

$$a^x = (a^{\operatorname{ord}_n a})^k \equiv 1 \pmod{n}.$$

(41) p. 309, Example 9.2: The congruence in the middle should be $2^x \equiv 1 \pmod{7}$, not $2x$.
(42) p. 312, Example 9.9: Should have $m = 11$.
(43) p. 313, Exercise 9.1.15: You need to indicate where r comes from. (The problem is false if $r = 0$!) We must start with $r \in \mathbb{Z}$ such that $\gcd(r, p) = 1$.
(44) p. 314: After Exercise 21, you should have "used for encrypt*ion* is know$n$".
(45) p. 317: Following Corollary 9.8.1, should have "not know$n$".
(46) p. 320, Exercise 9.2.16: False if $q = 2$ and $a = 2$. Also, why do you write $p - a^2$ instead of $-a^2$?
(47) p. 321: In the middle of the page, should have $p - 1 = \operatorname{ord}_r n$, not $\operatorname{ord}_p r$.
(48) p. 323: In the middle of the page, next to last paragraph, $\operatorname{ord}_{p^k} 5$ should be $\operatorname{ord}_{p^k} r$.

(49) p. 324: At the top of the page, in proving Theorem 9.10, you should indicate that the binomial theorem calculation is the critical moment where p odd is used.
(50) p. 324: Should have 7^2, not F^2.
(51) p. 325: At the top of the page, should have $a^{2^{k-1}} \equiv 1$.
(52) p. 325, Proof of Theorem 9.12: In the beginning of the proof, you miss the '1' in

$$5^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

(53) p. 326, Proof of Theorem 9.13: In the middle of the page, again you miss the '1'

$$r^U \equiv 1 \pmod{p_i^{t_i}}.$$

(54) p. 327, Proof of Theorem 9.14: At the start of the proof, you should have $r^{\phi(p^t)}$ in the indented equation, not $r^{\phi(p')}$.
(55) p. 329, Exercise 9.4.15: The statement is ambiguous. You should say "every odd integer is congruent *modulo* 2^k...".
(56) p. 329, Definition: It is weird to define $\text{ind}_r\, 1 = \phi(m)$ instead of $\text{ind}_r\, 1 = 0$. Better to take $0 \leq x < \phi(m)$. And again, why switch between m and n? Also, it is not necessary that r be a primitive root to define a discrete logarithm! All you need is that there exists an exponent x such that $r^x \equiv a \pmod{m}$.
(57) p. 338, Exercise 9.4.10: Should be "Prove that *there* are". Also, should be $(p_1 \cdot p_2 \cdots p_n)^4$, not $(p_1, p_2 \cdot p_n)^4$. And to make it simpler, you really should take $Q = (2p_1 \dots p_n)^4 + 1$, since then Q is odd.
(58) p. 340: On page 340, on the proof of Theorem 9.18, it says: $x^{(n-1)/q} = x^{k/(ord_n x \cdot q)}$. It should be $x^{(k \cdot ord_n(x))/q}$.
(59) p. 341, Theorem 9.19: In the statement, "such" should be "such that". The proof of Pocklington's test contains a misprint and a logical slip. The misprint occurs after the statement that $n-1 < F^2$ and that $n-1$ and F^2 are integers. We have $n \leq F^2$; you wrote $n-1 < F^2$. The slip occurs when you say that $F \mid ord_p(a)$ because all prime divisors of F divide $ord_p(a)$. This makes sense only if F is squarefree. In the example that you give on the next page, F is 200.
(60) p. 343: In the proof of Theorem 9.22, near the bottom of the page: For (i), it should be the prime-power factorization of $n-1 = 2^a q_1^{e_1} q_2^{e_2} \cdots q_t^{e^t}$. For (ii), it should probably also mention that q_i is an *odd* prime. For (iv), it should be $x^{(n-1)/q} \not\equiv 1 \pmod{n}$.
(61) p. 344: On the last line, the exponent $2n$ in the definition of F_n should be 2^n.
(62) p. 376: The definition of a quadratic nonresidue is confusing. We must have $\gcd(a,m) = 1$, but this qualifier appears only in the context of the definition of a quadratic residue.
(63) p. 376, Example 11.1: You should have $1^2 \equiv 10^2$ and $2^2 \equiv 9^2$.
(64) p. 376, Lemma 11.1: "[...] has either no solutions of exactly two *incongruent* solutions modulo p."
(65) p. 378: Why do you not define the Legendre symbol $(a/p) = 0$ if $p \mid a$? This is usual practice and requires minimal changes to your theorems. In the statement for Theorem 11.3, we do not need a to be positive.

(66) p. 379: Should say "By Theorem 4.10, for each integer i such that $\gcd(i, p) = 1$, *there is an integer* j such that $ij \equiv a \pmod{p}$.
(67) p. 387, Exercise 11.1.10: The numerator in the last Legendre symbol should be $(p-1)b$.
(68) p. 392, Theorem 11.7: Need p, q *distinct* odd primes.
(69) p. 397: In the example, just below Figure 11.1, in the second sentence you should have $1 \le x \le 3$, not $1 \le x \le 43$.
(70) p. 401, Exercise 11.2.1: The solutions in the back refer to the solution for Exercise 11.1.1.
(71) p. 414: Three lines from the bottom, just before the $\pmod{p}$ at the end of the line, there is $(p-1)/2^{r+c}$ which should read $(p-1)/(2^{r+1}c)$. On the next page, line 3, a_j should be a_i. Also on p. 415, the $\prod$ in the fourth displayed equation should be $\sum$.
(72) p. 417, Lemma 11.5: In the proof, "By Theorem 9.27" should read "By Theorem 9.24".
(73) p. 437, Theorem 12.5: should have $C > 0$; the assertion is vacuous if $C = -1$ or $C = 0$. Similarly, on p. 438, the inequality with $2/10^{(k+1)!}$ implies only that any C would have to be non-positive. Also, the notion of algebraic number "of degree n" is not defined (nor in §1.1).
(74) p. 444: In the first series of displayed equations, the first three left-hand-sides are botched: $r + i$ should be r_i for $i = 0, 1, 2$.
(75) p. 447: On the last line, $p_k p_{k-1} - q_k p_{k-1}$ should read $p_k q_{k-1} - q_k p_{k-1}$.
(76) p. 450, Exercise 12.2.10: Should have $a_0 > 0$ rather thatn $a_0 \neq 0$. The numbers in a continued fraction other than the 0th are positive (p. 443).
(77) p. 456: On the top few lines, the formula for $\alpha - C_k$ that you get needs to be multiplied by -1. In the middle of the three displayed formulas, the numerator has a minus sign. That sign seems to have been forgotten in the formula below it.
(78) p. 473: On line 6, "Note, however..." The exercise from section 12.2 is #10, not #6. In the two displayed equations that are part of this sentence, you have indices n that should be k.
(79) p. 463, Lemma 12.1: In the statement, the minus sign in the displayed equaton should be a $=$ sign.
(80) p. 542, factor table: Entries for 700–719 misprinted as 7700–7719.