Joshua Ferguson

Exercises 5.1, 5.3, 5.4, 6.1, 6.2, 6.5, possibly 6.6

5.1. Use the Euclidean algorithm to compute each of the following gcd's.

(a) gcd(12345,67890)

67890 = (5 x 12345) + 6165

12345 = (2 x 6165) + 15

6165 = (411 x 15) + 0

hence, the gcd is 15

(b) gcd(54321,9876)

54321 = (5 x 9876) + 4941

9876 = (1 x 4941) + 4935

4941 = (1 x 4935) + 6

4935 = (822 x 6) + 3

6 = (2 x 3) + 0

hence, the gcd is 3

5.3. Let $b = r_0, r_1, r_2, ...$ be the successive remainders in the Euclidean algorithm applied to a and b. Show that after every two steps, the remainder is reduced by at least one half. In other words, verify that $r_{i+2} < \frac{1}{2} r_i for\ every\ i = 0, 1, 2, ...$ Conclude that the Euclidean algorithm terminates in at most $2log_2(b)$ steps, where log_2 is the logarithm to the base 2. In particular, show that the number of steps is at most seven times the number of digits in b. [Hint. What is the value of $log_2(10)$?]

in the euclidean algorithm given 2 values x and y, let m and n be larger and smaller value respectively. there exists a q and r such that m=(q x n)+r. Then, so long as n is not 0, m is the previous value for n and n is the previous value for r.

let $r_i = r$ at the i^{th} step of the euclidean algorithm. then, since the value of $ri + 1$ is the remainder of some quotient and r_i then it follows that $r_i > r_{i+1}$

this means that if r_i is divided by r_{i+1} the result is a remander of $(r_i - q * r_{i+1})$ where $q \in Z$.

by the next step of the euclidean algorithm

$r_i = q * r_{i+1} + r_{i+2}$

$r_i - q * r_{i+1} = r_{i+2}$

now let us consider 2 cases:

if $r_i > 2r_{i+1}$, then:

then $q < 2$ and

$r_{i+2} < \frac{r_i}{2}$ is already proven.

else if $r_i > 2r_{i+1}$, then:

q=1 and r_{i+2} is at least $\frac{r_1}{2} - 1$ or q would be greater than 1

therefore, $r_{i+2} < \frac{r_i}{2}$

since the above shows that the the value of the remander is reduced by at least half every $2n$ steps, and that the first remainder is less than |b|, then we can say that $r_n < \frac{b}{2^n}$

since the remainder has to be an integer value, the value always has to be greater than or equal to 1,

$1 \leq \frac{b}{2^n}$

$b \leq 2^n$

now take the log_2 of both sides

$log_2 b \geq log_2 2^n$

$log_2 b \geq n$

hence the algorithm never takes more than $2log_2 b$ number of steps

in order to figure out n in terms of number of digits in b we need to convert from a log base 2 to a log base 10.

$$2log_2 b = \frac{2log_{10}b}{log_{10}2}$$

$$2log_2 b = \frac{2}{log_{10}2} log_{10}b$$

$$\approx 6.64 log_{10}b$$

since $log_{10}b$ is always greater than the number of digits in b, then n is at most 7 times the number of digits of b.

QED

5.4. A number L is called a common multiple of m and n if both m and n divide L.The smallest such L is called the least common multiple of m and n and is denoted by LCM(ra, n). For example, LCM(3, 7) = 21 and LCM(12,66) = 132.

(a) Find the following least common multiples.(i) LCM(8,12) (ii) LCM(20,30) (iii) LCM(51,68) (iv) LCM(23,18).

lcm(8,12)=24

lcm(20,30)=60

lcm(51,68)=204

lcm(23,18)=414

(b) For each of the LCMs that you computed in (a), compare the value of LCM(ra, n)to the values of m, n, and gcd(ra, n). Try to find a relationship.

I kind of figured this out on my in the first step.

if finding the lcm(a,b):

let m=max(a,b) and n=min(a,b),

then the $lcm = n \times (m \div gcd(a, b))$

(c) Give an argument proving that the relationship you found is correct for all m and n.

let r=gcd(a,b)

then m=r*k n=r*j where $k, j \in Z$

since r is the gcd of a and b, and by definition $m > n$,

then $k > j$

and $r * j * k$ is the first number that is a multiple of both values.

(d) Use your result in (b) to compute LCM(301337,307829).

171460753

(e) Suppose that gcd(ra, n) = 18 and LCM(ra, n) = 720. Find m and n. Is there morethan one possibility? If so, find all of them.

since 720 is $r * j * k$

720/18=40=$j * k$

values for (j,k):

8,5

4,10

2,20

1,40

values for a,b:

144,90

72,180

36,360

18,720

6.1.

(a) Find a solution in integers to the equation $12345x + 67890y = gcd(12345, 67890)$.

Finding the smallest possible solution to 12345x+67890y 6165 = a - 5*b 15 = -2*a + 11*b hence, the smallest linear solution is: -2*a + 11*b = 15 where a = 67890 and b = 12345 QED

(b) Find a solution in integers to the equation $54321x + 9876y = gcd(54321, 9876)$.

Finding the smallest possible solution to 54321x+9876y 4941 = a - 5*b 4935 = -a + 6*b 6 = 2*a - 11*b 3 = -1645*a + 9048*b hence, the smallest linear solution is: -1645*a + 9048*b = 3 where a = 54321 and b = 9876 QED

6.2. Describe all integer solutions to each of the following equations.

(a) $105x + 121y = 1$

the gcd is 1, hence 1 is the smallest possible solution

to get the values for x, and y which solve this solution let a, b be equal to the max and min of x and y respectively, then:

work through the euclidian algorithm to solve for the remainder:

Finding the smallest possible solution to 105x+121y

16 = a - b

9 = -6*a + 7*b

7 = 7*a - 8*b

2 = -13*a + 15*b

1 = 46*a - 53*b

hence, the smallest linear solution is: 46*a - 53*b = 1 where a = 121 and b = 105

via the linear equation theorem, all possible solutions can be find via the formulas:

105*k + 46 -121*k - 53

first 100 solution pairs:

(46 , -53) (151 , -174) (256 , -295) (361 , -416) (466 , -537) (571 , -658) (676 , -779) (781 , -900) (886 , -1021) (991 , -1142) (1096 , -1263) (1201 , -1384) (1306 , -1505) (1411 , -1626) (1516 , -1747) (1621 , -1868) (1726 , -1989) (1831 , -2110) (1936 , -2231) (2041 , -2352) (2146 , -2473) (2251 , -2594) (2356 , -2715) (2461 , -2836) (2566 , -2957) (2671 , -3078) (2776 , -3199) (2881 , -3320) (2986 , -3441) (

3091 , -3562) (3196 , -3683) (3301 , -3804) (3406 , -3925) (3511 , -4046) (3616 , -4167) (3721 , -4288) (3826 , -4409) (3931 , -4530) (4036 , -4651) (4141 , -4772) (4246 , -4893) (4351 , -5014) (4456 , -5135) (4561 , -5256) (4666 , -5377) (4771 , -5498) (4876 , -5619) (4981 , -5740) (5086 , -5861) (5191 , -5982) (5296 , -6103) (5401 , -6224) (5506 , -6345) (5611 , -6466) (5716 , -6587) (5821 , -6708) (5926 , -6829) (6031 , -6950) (6136 , -7071) (6241 , -7192) (6346 , -7313) (6451 , -7434) (6556 , -7555) (6661 , -7676) (6766 , -7797) (6871 , -7918) (6976 , -8039) (7081 , -8160) (7186 , -8281) (7291 , -8402) (7396 , -8523) (7501 , -8644) (7606 , -8765) (7711 , -8886) (7816 , -9007) (7921 , -9128) (8026 , -9249) (8131 , -9370) (8236 , -9491) (8341 , -9612) (8446 , -9733) (8551 , -9854) (8656 , -9975) (8761 , -10096) (8866 , -10217) (8971 , -10338) (9076 , -10459) (9181 , -10580) (9286 , -10701) (9391 , -10822) (9496 , -10943) (9601 , -11064) (9706 , -11185) (9811 , -11306) (9916 , -11427) (10021 , -11548) (10126 , -11669) (10231 , -11790) (10336 , -11911) (10441 , -12032)

(b) $12345x + 67890y = gcd(12345, 67890)$

continuing from 6.1(A):

hence, the smallest linear solution is: -2*a + 11*b = 15 where a = 67890 and b = 12345

via the linear equation theorem, all possible solutions can be find via the formulas:

823*k - 2 -4526*k + 11

first 100 solution pairs:

(-2 , 11) (821 , -4515) (1644 , -9041) (2467 , -13567) (3290 , -18093) (4113 , -22619) (4936 , -27145) (5759 , -31671) (6582 , -36197) (7405 , -40723) (8228 , -45249) (9051 , -49775) (9874 , -54301) (10697 , -58827) (11520 , -63353) (12343 , -67879) (13166 , -72405) (13989 , -76931) (14812 , -81457) (15635 , -85983) (16458 , -90509) (17281 , -95035) (18104 , -99561) (18927 , -104087) (19750 , -108613) (20573 , -113139) (21396 , -117665) (22219 , -122191) (23042 , -126717) (23865 , -131243) (24688 , -135769) (25511 , -140295) (26334 , -144821) (27157 , -149347) (27980 , -153873) (28803 , -158399) (29626 , -162925) (30449 , -167451) (31272 , -171977) (32095 , -176503) (32918 , -181029) (33741 , -185555) (34564 , -190081) (35387 , -194607) (36210 , -199133) (37033 , -203659) (37856 , -208185) (38679 , -212711) (39502 , -217237) (40325 , -221763) (41148 , -226289) (41971 , -230815) (42794 , -235341) (43617 , -239867) (44440 , -244393) (45263 , -248919) (46086 , -253445) (46909 , -257971) (47732 , -262497) (48555 , -267023) (49378 , -271549) (50201 , -276075) (51024 , -280601) (51847 , -285127) (52670 , -289653) (53493 , -294179) (54316 , -298705) (55139 , -303231) (55962 , -307757) (56785 , -312283) (57608 , -316809) (58431 , -321335) (59254 , -325861) (60077 , -330387) (60900 , -334913) (61723 , -339439) (62546 , -343965) (63369 , -348491) (64192 , -353017) (65015 , -357543) (65838 , -362069) (66661 , -366595) (67484 , -371121) (68307 , -375647) (69130 , -380173) (69953 , -384699) (70776 , -389225) (71599 , -393751) (72422 , -398277) (73245 , -402803) (74068 , -407329) (74891 , -411855) (75714 , -416381) (76537 , -420907) (77360 , -425433) (78183 , -429959) (79006 , -434485) (79829 , -439011) (80652 , -443537) (81475 , -448063)

(c) $54321x + 9876y = gcd(54321, 9876)$

continuing from 6.1 b

hence, the smallest linear solution is: -1645*a + 9048*b = 3 where a = 54321 and b = 9876

via the linear equation theorem, all possible solutions can be find via the formulas:

$3292k - 1645 -18107k + 9048$

first 100 solution pairs:

(-1645 , 9048) (1647 , -9059) (4939 , -27166) (8231 , -45273) (11523 , -63380) (14815 , -81487) (18107 , -99594) (21399 , -117701) (24691 , -135808) (27983 , -153915) (31275 , -172022) (34567 , -190129) (37859 , -208236) (41151 , -226343) (44443 , -244450) (47735 , -262557) (51027 , -280664) (54319 , -298771) (57611 , -316878) (60903 , -334985) (64195 , -353092) (67487 , -371199) (70779 , -389306) (74071 , -407413) (77363 , -425520) (80655 , -443627) (83947 , -461734) (87239 , -479841) (90531 , -497948) (93823 , -516055) (97115 , -534162) (100407 , -552269) (103699 , -570376) (106991 , -588483) (110283 , -606590) (113575 , -624697) (116867 , -642804) (120159 , -660911) (123451 , -679018) (126743 , -697125) (130035 , -715232) (133327 , -733339) (136619 , -751446) (139911 , -769553) (143203 , -787660) (146495 , -805767) (149787 , -823874) (153079 , -841981) (156371 , -860088) (159663 , -878195) (162955 , -896302) (166247 , -914409) (169539 , -932516) (172831 , -950623) (176123 , -968730) (179415 , -986837) (182707 , -1004944) (185999 , -1023051) (189291 , -1041158) (192583 , -1059265) (195875 , -1077372) (199167 , -1095479) (202459 , -1113586) (205751 , -1131693) (209043 , -1149800) (212335 , -1167907) (215627 , -1186014) (218919 , -1204121) (222211 , -1222228) (225503 , -1240335) (228795 , -1258442) (232087 , -1276549) (235379 , -1294656) (238671 , -1312763) (241963 , -1330870) (245255 , -1348977) (248547 , -1367084) (251839 , -1385191) (255131 , -1403298) (258423 , -1421405) (261715 , -1439512) (265007 , -1457619) (268299 , -1475726) (271591 , -1493833) (274883 , -1511940) (278175 , -1530047) (281467 , -1548154) (284759 , -1566261) (288051 , -1584368) (291343 , -1602475) (294635 , -1620582) (297927 , -1638689) (301219 , -1656796) (304511 , -1674903) (307803 , -1693010) (311095 , -1711117) (314387 , -1729224) (317679 , -1747331) (320971 , -1765438) (324263 , -1783545)

6.5. Suppose that gcd(a, b) = 1. Prove that for every integer c, the equation ax + by = c has a solution in integers x and y. [Hint. Find a solution to au + bv = 1 and multiply by c] Find a solution to 37x + 47y = 103. Try to make x and y as small as possible.

first lets find the gcd of (a,b)

by definition the greatest common divisor of a,b will be the largest positive number that divides both a and b without remainder

let $ p,q,x,y, c \in Z$

by the euclidean algorithm,

ap+bq=gcd(a,b)

since the gcd(a,b)=1

then,

ap+bq=1

multiply both sides by the constant c:

apc+bqc=c

let x=pc & y=qc,

Finding the gcd of 37 and 47 using the euclidean algorithm 47 = (1 x 37) + 10 37 = (3 x 10) + 7 10 = (1 x 7) + 3 7 = (2 x 3) + 1 3 = (3 x 1) + 0 hence, the gcd is 1 Finding the smallest possible solution to 37x+47y 10 = a - b 7 = -3*a + 4*b 3 = 4*a - 5*b 1 = -11*a + 14*b hence, the smallest linear solution is: -11*a + 14*b = 1 where a = 47 and b = 37

since c is 103 in 37x+47y=103

x=pc=14*103=1442

y=qc=-11*103=-1133

with a=37 and b=47

ax+by=103

thus the smallest solution is found

QED