Number Theory Proofs

Mayank Agrawal, Jeffrey Hahm, Alexander Kiehn, Michael Wong, Brian Xu

February 2014

1 Solutions to Euclid's Algorithm

Q 1.0.1

$gcd(9,15)$

$= gcd(9,15\text{-}9)$

$= gcd(9,6)$

$= 3$

Q 1.0.2

$gcd(931, 946)$

$= gcd(931, 946 - 931)$

$= gcd(931, 15)$

$= 1$

Q 1.0.3

$gcd(836, 957)$

$= gcd(836, 957 - 836)$

$= gcd(836, 121)$

$= 11$

Q 1.0.4

$gcd(7645389,7635389)$

$= gcd(7645389\text{-}7635389,7635389)$

$= gcd(10000,7635389)$

$10000=2^4 * 5^4$

$2 \nmid 7635389$ and $5 \nmid 7635389$.

$\therefore gcd(10000,7635389)=1$, so $gcd(7645389,7635389)=1$

Q 1.0.5

$gcd(205,101)$

$= gcd(205\text{-}101,101)$

$= gcd(104,101)$

= gcd(104-101,101)

= gcd(3,101)

= 3

Q 1.0.6

gcd(135,271)

= gcd(135,271-135)

= gcd(135,136)

= gcd(135,136-135)

= gcd(135,1)

= 1

Q 1.0.7

= gcd(289, 165)

= gcd(289-165, 165)

= gcd(124, 165)

= 1

Q 1.0.8

gcd(21, 24, 27)

= gcd(21, 24 - 21, 27 - 21)

= gcd(21, 3, 3)

= 3

Q 1.0.9

gcd(30,24,22)

=gcd(8,2,22)

=gcd(8,2,6)

=2

Q 1.0.10

gcd(N,N)= N

gcd(N,N+1)= 1

gcd(N,N+2)

When 2|N, gcd(N,N+2)=2

When $2 \nmid N$, $gcd(N, N+2) = 1$

gcd(N,N+3)

When 3|N, gcd(N,N+3)=3

When $3 \nmid N$, $gcd(N, N+3) = 1$

gcd(N,N+4)

When 4|N, gcd(N,N+4)=4

When 2|N and $N \nmid 4$, $gcd(N, N+4) = 2$

When $2 \nmid N$, $gcd(N, N+4) = 1$

Q 1.0.11

gcd(3N+1,3N+4)

= gcd((3N+1,[3N+4]-[3N+1])

= gcd(3N+1,3)

= gcd(3N+1-3N,3) Use Euclid's algorithm to subtract "3" N times

= gcd(1,3)

=1

Q 1.0.12

If N > P, the gcd P

If N = P, the gcd = N

If N < P, the gcd $\leq N$

Q 1.0.13

gcd(2N, N + P)

= gcd(2N - [N + P], N + P)

= gcd(N - P, N + P)

= gcd(N + P, N + P - [N - P])

$= gcd(\text{N} + \text{P}, 2\text{P})$

if $\text{P} \mid \text{N}, gcd = P$

if $\text{P} \nmid \text{N}$ and $2 \mid \text{N}, gcd = 2$

if $\text{P} \nmid \text{N}$ and $2 \nmid \text{N}, gcd = 1$

Q 1.0.14

gcd(4,16)=4

gcd(13,52)=13

Q 1.0.15

$gcd(2^1 3^2 5^3, 2^3 3^2 5^1)$

$= 2^1 3^2 5^1$

Q 1.0.16

$gcd(7^2 11^{47}, 3^1 7^{567} 11^3)$

$= 7^2 11^3$

Q 1.0.17

$gcd(2^3 5^1 7^8, 5^2 7^1 13^3)$

$= 5^1 7^1$

Q 1.0.18

$gcd(2^1 3^2 5^1 11^6, 2^1 3^0 5^2 7^1 11^{73})$

$= 2^1 3^0 5^1 11^6$

Q 1.0.19

gcd(M,N)

$=(2^{min(e_2,f_2)})(3^{min(e_3,f_3)})(5^{min(e_5,f_5)})...$

Q 1.0.20

$lcm\ (2^3 5^1 7^8, 5^2 7^1 13^3)$

$= 2^3 5^2 7^8 13^3$

Q 1.0.21

$lcm(2^1 3^2 5^1 11^6, 2^1 3^0 5^2 7^1 11^{73})$

$= 2^1 3^2 5^2 7^1 11^{73}$

Q 1.0.22

-*lcm* (N,M)

$=(2^{max(e_2,f_2)})(3^{max(e_3,f_3)})(5^{max(e_5,f_5)})...$

-[*gcd* (N,M)][*lcm* (N,M)]

$=(2^{e_2 f_2})(3^{e_3 f_3})(5^{e_5 f_5})...$

=NM

-*lcm* (N,M)

"Find the gcd"

"Divide NM by gcd"

1.1 The Algorithm

Q 1.1.1

gcd(87452, 52584)

$= gcd$(34868, 52584)

$= gcd$(34868, 17716)

$= gcd$(17152, 17716)

$= gcd$(564, 17716)

$= gcd$(564, 232)

$= gcd$(100, 232)

$= gcd$(100, 32)

$= gcd$(32, 4)

$= 4$

Q 1.1.2

gcd(15646, 5124)

$= gcd$(274,5124)

$= gcd$(274,192)

$= gcd(82,192)$

$= gcd(82,28)$

$= gcd(26,28)$

$= 2$

Q 1.1.3

$gcd(0.4,\ 3)$

$= gcd(0.4,\ 0.2)$

$= 0.2$

Q 1.1.4

$gcd(\sqrt{1}8, \sqrt{8})$

$= gcd(3\sqrt{2}, 2\sqrt{2})$

$= gcd(\sqrt{2}, 2\sqrt{2})$

$= \sqrt{2}$

Q 1.1.5

$gcd(3,\sqrt{2})$

$r_1 = 3$

$r_2 = \sqrt{2}$

$r_3 \approx .17157 \qquad 3 = 2 * \sqrt{2} + .17157$

$r_4 \approx .04163 \qquad \sqrt{2} = 8 * .17157 + .04163$

$r_5 \approx .00505 \qquad .17157 = 4 * .04163 + .005$

...

The algorithm never ends, and since the gcd is the last non-zero remainder, then the gcd does not exist for these two numbers.

Q 1.1.6

$gcd(F_{n+1}, F_n)$

$r_1 = F_{n+1}$

$r_2 = F_n$

$r_3 = F_{n-1}$

...

$r_{n+1} = F_1 = 1$

$r_{n+2} = F_0 = 0$

$\therefore gcd(F_{n+1}, F_n) = 1$

Q 1.1.7

$gcd(F_{n+2}, F_n)$

$r_1 = F_{n+2}$

$r_2 = F_n$

$r_3 = F_{n-1} \qquad F_{n+2} = 2F_n + F_{n-1}$

$gcd(F_n, F_{n-1}) = 1$

Q 1.1.8

We can separate this into three cases: n = 3k, n = 3k+1 and n = 3k+2

Case 1: n = 3k.

Let's try an inductive argument.

Inductive hypothesis: Assume that $gcd(F_{3k}, F_{3k+3}) = 2$

Base Case: $gcd(F_3, F_6) = gcd(2, 8) = 2$

Proof: Set $F_{3k} = x$ and $F_{3k+1} = y$

Therefore, $F_{3k+2} = x + y, ...F_{3k+3} = 2y + x, ...F_{3k+6} = 8y + 5x.$

We know that $gcd($ x, 2y + x$) = 2$. Using Euclid's algorithm four times, we get that

$gcd($2y + x, 8y+5x$) = gcd($2y + x, x$) = 2$.

Do the same induction argument for cases n = 3k+1 and n = 3k+2, except the gcd will be one instead of two.

Q 1.1.9

gcd(93,15) leaves behind a relatively small remainder term, so there are few steps. On the other hand, the remainder term when applying the algorithm to gcd(93,57) is larger, so there will be more steps and the algorithm will be work more slowly.

Q 1.1.10

Euclid's algorithm works slowest if A and B are somewhere in between. If A and B are nearly equal, the remainder will be small, so there will be few steps. Similarly, if one is much smaller than the other, then the remainder will be small, leading to relatively fewer steps. Thus, when A and B are an intermediate distance away, the algorithm will work the slowest. For the second half of the question, let us try to construct a worst case scenario working backwards.

The last step, since we're trying to construct a case with the most steps will be gcd(0,1)

Working backwards, we can construct the worst case by just adding the larger term to the smaller term. This will be the worst case because it maximizes the number of steps to get to a number.

gcd(0,1)

gcd(1,1)

gcd(2,1)

gcd(2,3)

gcd(5,3)

gcd(5,8)

...

In general, the worst case scenario will be occur when the two numbers take the form of $gcd(F_n, F_{n+1})$

Q 1.1.11

For all positive integers N, let k be the smallest positive integer such that $F_k < N$.

There exists a k such that the kth Fibonnaci term is less than N which is less than or equal to a (k+1)th Fibonnaci term. Since Euclid's algorithm is slowest for consecutive Fibonnaci terms, the maximum number of steps required to determine the gcd(A,B) such that A,B < N will occur when A,B are F_k, F_{k-1},

$\therefore$ maximum number of steps is k-1