

FCS Math 0 Second Lesson

The Euclidean Algorithm with Simplification Tricks

The basic step and the tricks

The plain Euclidean algorithm repeatedly replaces (a, b) by (b, r) , where $a = qb + r$, using

$$\gcd(a, b) = \gcd(b, a - qb) \quad \text{for every integer } q.$$

The following facts allow us to shorten the computation considerably. At every stage we keep the gcd in the form $m \cdot \gcd(a, b)$, where m collects the factors already extracted.

1. **Divisibility check.** If $b \mid a$ then $\gcd(a, b) = b$. It is worth checking before every division.
2. **Prime check.** If b is prime, then $\gcd(a, b) = b$ if $b \mid a$ and $\gcd(a, b) = 1$ otherwise. In particular $\gcd(a, 1) = 1$.
3. **Common factors.** For every $k \geq 1$,

$$\gcd(ka, kb) = k \gcd(a, b).$$

So a factor visibly dividing both numbers can be pulled out immediately.

4. **Useless factors.** If p is prime, $p \mid a$ and $p \nmid b$, then p does not divide $\gcd(a, b)$, hence

$$\gcd(a, b) = \gcd(a/p, b).$$

Factors that appear in only one of the two numbers can therefore be cancelled.

5. **Least absolute remainder.** Since q in $\gcd(a, b) = \gcd(b, a - qb)$ is arbitrary and $\gcd(b, -r) = \gcd(b, r)$, we may choose q so that $|a - qb| \leq b/2$: if the ordinary remainder r exceeds $b/2$, use $q + 1$ and the negative remainder $r - b$ instead. The numbers then at least halve at each division.

Divisibility criteria used. A number is divisible by 2 if it ends in an even digit; by 5 if it ends in 0 or 5; by 10 if it ends in 0; by 3 if its digit sum is divisible by 3; by 11 if its alternating digit sum (from the right: units – tens + hundreds – ...) is divisible by 11.

Order of operations. In the examples we apply, in this order: the divisibility and prime checks, the extraction of common factors, the cancellation of useless factors, and only then a division with least absolute remainder. After each step the current state is displayed as $m \cdot \gcd(a, b)$, with $a \geq b$.

1 Two- and three-digit numbers

Example 1: $\gcd(54, 84)$

1. *Common factor:* $p = 2$ divides both, since 84 ends in 4 and 54 ends in 4. Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(54, 84) = 2 \cdot \gcd(27, 42).$$

2. *Common factor:* $p = 3$ divides both, since the digit sum of 42 is $4 + 2 = 6$ and the digit sum of 27 is $2 + 7 = 9$. Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(54, 84) = 6 \cdot \gcd(14, 9).$$

3. *Remove a useless factor:* 2 divides 14 (14 ends in 4) but not 9 (9 ends in 9), so 2 cannot divide the gcd and we may cancel it from 14: $14 = 2 \cdot 7$.

$$\gcd(54, 84) = 6 \cdot \gcd(9, 7).$$

4. *Prime check:* 7 is prime and does not divide 9, so $\gcd(9, 7) = 1$.

$$\gcd(54, 84) = 6 \cdot 1 = 6.$$

$$\boxed{\gcd(54, 84) = 6}$$

Comparison: 0 divisions with the tricks, against 4 in the plain Euclidean algorithm.

Example 2: $\gcd(95, 18)$

1. *Remove a useless factor:* 2 divides 18 (18 ends in 8) but not 95 (95 ends in 5), so 2 cannot divide the gcd and we may cancel it from 18: $18 = 2 \cdot 9$.

$$\gcd(95, 18) = \gcd(95, 9).$$

2. *Remove a useless factor:* 5 divides 95 (95 ends in 5) but not 9 (9 ends in 9), so 5 cannot divide the gcd and we may cancel it from 95: $95 = 5 \cdot 19$.

$$\gcd(95, 18) = \gcd(19, 9).$$

3. *Remove a useless factor:* 3 divides 9 (9 is a multiple of 3) but not 19 (the digit sum of 19 is 10, not a multiple of 3), so 3 cannot divide the gcd and we may cancel 3^2 from 9: $9 = 9 \cdot 1$.

$$\gcd(95, 18) = \gcd(19, 1).$$

4. One of the two numbers is 1, so the remaining gcd is 1.

$$\boxed{\gcd(95, 18) = 1}$$

Comparison: 0 divisions with the tricks, against 5 in the plain Euclidean algorithm.

Example 3: $\gcd(85, 34)$

1. *Remove a useless factor:* 2 divides 34 (34 ends in 4) but not 85 (85 ends in 5), so 2 cannot divide the gcd and we may cancel it from 34: $34 = 2 \cdot 17$.

$$\gcd(85, 34) = \gcd(85, 17).$$

2. *Divisibility check:* 17 divides 85 ($85 = 5 \cdot 17$), so $\gcd(85, 17) = 17$.

$$\boxed{\gcd(85, 34) = 17}$$

Comparison: 0 divisions with the tricks, against 2 in the plain Euclidean algorithm.

Example 4: $\gcd(952, 697)$

1. *Remove a useless factor:* 2 divides 952 (952 ends in 2) but not 697 (697 ends in 7), so 2 cannot divide the gcd and we may cancel 2^3 from 952: $952 = 8 \cdot 119$.

$$\gcd(952, 697) = \gcd(697, 119).$$

2. *Division with least absolute remainder:* $697 = 6 \cdot 119 - 17$. Using the *negative* remainder -17 (since $17 < 119 - 17$) gives a smaller number, and $\gcd(697, 119) = \gcd(119, 17)$ because signs do not affect the gcd.

$$\gcd(952, 697) = \gcd(119, 17).$$

3. *Divisibility check:* 17 divides 119 ($119 = 7 \cdot 17$), so $\gcd(119, 17) = 17$.

$$\boxed{\gcd(952, 697) = 17}$$

Comparison: 1 division with the tricks, against 6 in the plain Euclidean algorithm.

Example 5: $\gcd(338, 767)$

1. *Remove a useless factor:* 2 divides 338 (338 ends in 8) but not 767 (767 ends in 7), so 2 cannot divide the gcd and we may cancel it from 338: $338 = 2 \cdot 169$.

$$\gcd(338, 767) = \gcd(767, 169).$$

2. *Division with least absolute remainder:* $767 = 5 \cdot 169 - 78$. Using the *negative* remainder -78 (since $78 < 169 - 78$) gives a smaller number, and $\gcd(767, 169) = \gcd(169, 78)$ because signs do not affect the gcd.

$$\gcd(338, 767) = \gcd(169, 78).$$

3. *Remove a useless factor:* 2 divides 78 (78 ends in 8) but not 169 (169 ends in 9), so 2 cannot divide the gcd and we may cancel it from 78: $78 = 2 \cdot 39$.

$$\gcd(338, 767) = \gcd(169, 39).$$

4. *Remove a useless factor:* 3 divides 39 (the digit sum of 39 is $3 + 9 = 12$) but not 169 (the digit sum of 169 is 16, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 39: $39 = 3 \cdot 13$.

$$\gcd(338, 767) = \gcd(169, 13).$$

5. *Divisibility check:* 13 divides 169 ($169 = 13 \cdot 13$), so $\gcd(169, 13) = 13$.

$$\boxed{\gcd(338, 767) = 13}$$

Comparison: 1 division with the tricks, against 5 in the plain Euclidean algorithm.

Example 6: $\gcd(980, 385)$

1. *Common factor:* $p = 5$ divides both, since 980 ends in 0 and 385 ends in 5. Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(980, 385) = 5 \cdot \gcd(196, 77).$$

2. *Remove a useless factor:* 2 divides 196 (196 ends in 6) but not 77 (77 ends in 7), so 2 cannot divide the gcd and we may cancel 2^2 from 196: $196 = 4 \cdot 49$.

$$\gcd(980, 385) = 5 \cdot \gcd(77, 49).$$

3. *Division with least absolute remainder:* $77 = 2 \cdot 49 - 21$. Using the *negative* remainder -21 (since $21 < 49 - 21$) gives a smaller number, and $\gcd(77, 49) = \gcd(49, 21)$ because signs do not affect the gcd.

$$\gcd(980, 385) = 5 \cdot \gcd(49, 21).$$

4. *Remove a useless factor:* 3 divides 21 (the digit sum of 21 is $2 + 1 = 3$) but not 49 (the digit sum of 49 is 13, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 21: $21 = 3 \cdot 7$.

$$\gcd(980, 385) = 5 \cdot \gcd(49, 7).$$

5. *Divisibility check:* 7 divides 49 ($49 = 7 \cdot 7$), so $\gcd(49, 7) = 7$.

$$\gcd(980, 385) = 5 \cdot 7 = 35.$$

$\gcd(980, 385) = 35$

Comparison: 1 division with the tricks, against 4 in the plain Euclidean algorithm.

Example 7: $\gcd(434, 784)$

1. *Common factor:* $p = 2$ divides both, since 784 ends in 4 and 434 ends in 4. Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(434, 784) = 2 \cdot \gcd(392, 217).$$

2. *Remove a useless factor:* 2 divides 392 (392 ends in 2) but not 217 (217 ends in 7), so 2 cannot divide the gcd and we may cancel 2^3 from 392: $392 = 8 \cdot 49$.

$$\gcd(434, 784) = 2 \cdot \gcd(217, 49).$$

3. *Division:* $217 = 4 \cdot 49 + 21$, and $21 \leq 49/2$ is already the least absolute remainder.

$$\gcd(434, 784) = 2 \cdot \gcd(49, 21).$$

4. *Remove a useless factor:* 3 divides 21 (the digit sum of 21 is $2 + 1 = 3$) but not 49 (the digit sum of 49 is 13, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 21: $21 = 3 \cdot 7$.

$$\gcd(434, 784) = 2 \cdot \gcd(49, 7).$$

5. *Divisibility check:* 7 divides 49 ($49 = 7 \cdot 7$), so $\gcd(49, 7) = 7$.

$$\gcd(434, 784) = 2 \cdot 7 = 14.$$

$\gcd(434, 784) = 14$

Comparison: 1 division with the tricks, against 4 in the plain Euclidean algorithm.

Example 8: $\gcd(759, 913)$

1. *Common factor:* $p = 11$ divides both, since the alternating digit sum of 913 is 11 and the alternating digit sum of 759 is 11. Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(759, 913) = 11 \cdot \gcd(83, 69).$$

2. *Remove a useless factor:* 3 divides 69 (the digit sum of 69 is $6 + 9 = 15$) but not 83 (the digit sum of 83 is 11, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 69: $69 = 3 \cdot 23$.

$$\gcd(759, 913) = 11 \cdot \gcd(83, 23).$$

3. *Prime check:* 23 is prime and does not divide 83, so $\gcd(83, 23) = 1$.

$$\gcd(759, 913) = 11 \cdot 1 = 11.$$

$$\boxed{\gcd(759, 913) = 11}$$

Comparison: 0 divisions with the tricks, against 4 in the plain Euclidean algorithm.

Example 9: $\gcd(682, 800)$

1. *Common factor:* $p = 2$ divides both, since 800 ends in 0 and 682 ends in 2. Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(682, 800) = 2 \cdot \gcd(400, 341).$$

2. *Remove a useless factor:* 2 divides 400 (400 ends in 0) but not 341 (341 ends in 1), so 2 cannot divide the gcd and we may cancel 2^4 from 400: $400 = 16 \cdot 25$.

$$\gcd(682, 800) = 2 \cdot \gcd(341, 25).$$

3. *Remove a useless factor:* 5 divides 25 (25 ends in 5) but not 341 (341 ends in 1), so 5 cannot divide the gcd and we may cancel 5^2 from 25: $25 = 5 \cdot 5$.

$$\gcd(682, 800) = 2 \cdot \gcd(341, 1).$$

4. One of the two numbers is 1, so the remaining gcd is 1.

$$\gcd(682, 800) = 2 \cdot 1 = 2.$$

$$\boxed{\gcd(682, 800) = 2}$$

Comparison: 0 divisions with the tricks, against 7 in the plain Euclidean algorithm.

Example 10: $\gcd(791, 539)$

1. *Division:* $791 = 1 \cdot 539 + 252$, and $252 \leq 539/2$ is already the least absolute remainder.

$$\gcd(791, 539) = \gcd(539, 252).$$

2. *Remove a useless factor:* 2 divides 252 (252 ends in 2) but not 539 (539 ends in 9), so 2 cannot divide the gcd and we may cancel 2^2 from 252: $252 = 4 \cdot 63$.

$$\gcd(791, 539) = \gcd(539, 63).$$

3. *Remove a useless factor:* 3 divides 63 (the digit sum of 63 is $6 + 3 = 9$) but not 539 (the digit sum of 539 is 17, not a multiple of 3), so 3 cannot divide the gcd and we may cancel 3^2 from 63: $63 = 9 \cdot 7$.

$$\gcd(791, 539) = \gcd(539, 7).$$

4. *Divisibility check:* 7 divides 539 ($539 = 77 \cdot 7$), so $\gcd(539, 7) = 7$.

$$\boxed{\gcd(791, 539) = 7}$$

Comparison: 1 division with the tricks, against 4 in the plain Euclidean algorithm.

2 Four-digit numbers

Example 11: $\gcd(6162, 3562)$

1. *Common factor:* $p = 2$ divides both, since 6162 ends in 2 and 3562 ends in 2. Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(6162, 3562) = 2 \cdot \gcd(3081, 1781).$$

2. *Remove a useless factor:* 3 divides 3081 (the digit sum of 3081 is $3 + 0 + 8 + 1 = 12$) but not 1781 (the digit sum of 1781 is 17, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 3081: $3081 = 3 \cdot 1027$.

$$\gcd(6162, 3562) = 2 \cdot \gcd(1781, 1027).$$

3. *Division with least absolute remainder:* $1781 = 2 \cdot 1027 - 273$. Using the *negative* remainder -273 (since $273 < 1027 - 273$) gives a smaller number, and $\gcd(1781, 1027) = \gcd(1027, 273)$ because signs do not affect the gcd.

$$\gcd(6162, 3562) = 2 \cdot \gcd(1027, 273).$$

4. *Remove a useless factor:* 3 divides 273 (the digit sum of 273 is $2 + 7 + 3 = 12$) but not 1027 (the digit sum of 1027 is 10, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 273: $273 = 3 \cdot 91$.

$$\gcd(6162, 3562) = 2 \cdot \gcd(1027, 91).$$

5. *Division:* $1027 = 11 \cdot 91 + 26$, and $26 \leq 91/2$ is already the least absolute remainder.

$$\gcd(6162, 3562) = 2 \cdot \gcd(91, 26).$$

6. *Remove a useless factor:* 2 divides 26 (26 ends in 6) but not 91 (91 ends in 1), so 2 cannot divide the gcd and we may cancel it from 26: $26 = 2 \cdot 13$.

$$\gcd(6162, 3562) = 2 \cdot \gcd(91, 13).$$

7. *Divisibility check:* 13 divides 91 ($91 = 7 \cdot 13$), so $\gcd(91, 13) = 13$.

$$\gcd(6162, 3562) = 2 \cdot 13 = 26.$$

$$\boxed{\gcd(6162, 3562) = 26}$$

Comparison: 2 divisions with the tricks, against 8 in the plain Euclidean algorithm.

Example 12: $\gcd(7372, 5966)$

1. *Common factor:* $p = 2$ divides both, since 7372 ends in 2 and 5966 ends in 6. Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(7372, 5966) = 2 \cdot \gcd(3686, 2983).$$

2. *Remove a useless factor:* 2 divides 3686 (3686 ends in 6) but not 2983 (2983 ends in 3), so 2 cannot divide the gcd and we may cancel it from 3686: $3686 = 2 \cdot 1843$.

$$\gcd(7372, 5966) = 2 \cdot \gcd(2983, 1843).$$

3. *Division with least absolute remainder:* $2983 = 2 \cdot 1843 - 703$. Using the *negative* remainder -703 (since $703 < 1843 - 703$) gives a smaller number, and $\gcd(2983, 1843) = \gcd(1843, 703)$ because signs do not affect the gcd.

$$\gcd(7372, 5966) = 2 \cdot \gcd(1843, 703).$$

4. *Division with least absolute remainder:* $1843 = 3 \cdot 703 - 266$. Using the *negative* remainder -266 (since $266 < 703 - 266$) gives a smaller number, and $\gcd(1843, 703) = \gcd(703, 266)$ because signs do not affect the gcd.

$$\gcd(7372, 5966) = 2 \cdot \gcd(703, 266).$$

5. *Remove a useless factor:* 2 divides 266 (266 ends in 6) but not 703 (703 ends in 3), so 2 cannot divide the gcd and we may cancel it from 266: $266 = 2 \cdot 133$.

$$\gcd(7372, 5966) = 2 \cdot \gcd(703, 133).$$

6. *Division:* $703 = 5 \cdot 133 + 38$, and $38 \leq 133/2$ is already the least absolute remainder.

$$\gcd(7372, 5966) = 2 \cdot \gcd(133, 38).$$

7. *Remove a useless factor:* 2 divides 38 (38 ends in 8) but not 133 (133 ends in 3), so 2 cannot divide the gcd and we may cancel it from 38: $38 = 2 \cdot 19$.

$$\gcd(7372, 5966) = 2 \cdot \gcd(133, 19).$$

8. *Divisibility check:* 19 divides 133 ($133 = 7 \cdot 19$), so $\gcd(133, 19) = 19$.

$$\gcd(7372, 5966) = 2 \cdot 19 = 38.$$

$\gcd(7372, 5966) = 38$

Comparison: 3 divisions with the tricks, against 4 in the plain Euclidean algorithm.

Example 13: $\gcd(3052, 5124)$

1. *Common factor:* $p = 2$ divides both, since 5124 ends in 4 and 3052 ends in 2 (in fact 4 divides both). Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(3052, 5124) = 4 \cdot \gcd(1281, 763).$$

2. *Remove a useless factor:* 3 divides 1281 (the digit sum of 1281 is $1 + 2 + 8 + 1 = 12$) but not 763 (the digit sum of 763 is 16, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 1281: $1281 = 3 \cdot 427$.

$$\gcd(3052, 5124) = 4 \cdot \gcd(763, 427).$$

3. *Division with least absolute remainder:* $763 = 2 \cdot 427 - 91$. Using the *negative* remainder -91 (since $91 < 427 - 91$) gives a smaller number, and $\gcd(763, 427) = \gcd(427, 91)$ because signs do not affect the gcd.

$$\gcd(3052, 5124) = 4 \cdot \gcd(427, 91).$$

4. *Division with least absolute remainder:* $427 = 5 \cdot 91 - 28$. Using the *negative* remainder -28 (since $28 < 91 - 28$) gives a smaller number, and $\gcd(427, 91) = \gcd(91, 28)$ because signs do not affect the gcd.

$$\gcd(3052, 5124) = 4 \cdot \gcd(91, 28).$$

5. *Remove a useless factor:* 2 divides 28 (28 ends in 8) but not 91 (91 ends in 1), so 2 cannot divide the gcd and we may cancel 2^2 from 28: $28 = 4 \cdot 7$.

$$\gcd(3052, 5124) = 4 \cdot \gcd(91, 7).$$

6. *Divisibility check:* 7 divides 91 ($91 = 13 \cdot 7$), so $\gcd(91, 7) = 7$.

$$\gcd(3052, 5124) = 4 \cdot 7 = 28.$$

$\gcd(3052, 5124) = 28$

Comparison: 2 divisions with the tricks, against 6 in the plain Euclidean algorithm.

Example 14: $\gcd(6594, 2987)$

1. *Remove a useless factor:* 2 divides 6594 (6594 ends in 4) but not 2987 (2987 ends in 7), so 2 cannot divide the gcd and we may cancel it from 6594: $6594 = 2 \cdot 3297$.

$$\gcd(6594, 2987) = \gcd(3297, 2987).$$

2. *Remove a useless factor:* 3 divides 3297 (the digit sum of 3297 is $3 + 2 + 9 + 7 = 21$) but not 2987 (the digit sum of 2987 is 26, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 3297: $3297 = 3 \cdot 1099$.

$$\gcd(6594, 2987) = \gcd(2987, 1099).$$

3. *Division with least absolute remainder:* $2987 = 3 \cdot 1099 - 310$. Using the *negative* remainder -310 (since $310 < 1099 - 310$) gives a smaller number, and $\gcd(2987, 1099) = \gcd(1099, 310)$ because signs do not affect the gcd.

$$\gcd(6594, 2987) = \gcd(1099, 310).$$

4. *Remove a useless factor:* 2 divides 310 (310 ends in 0) but not 1099 (1099 ends in 9), so 2 cannot divide the gcd and we may cancel it from 310: $310 = 2 \cdot 155$.

$$\gcd(6594, 2987) = \gcd(1099, 155).$$

5. *Remove a useless factor:* 5 divides 155 (155 ends in 5) but not 1099 (1099 ends in 9), so 5 cannot divide the gcd and we may cancel it from 155: $155 = 5 \cdot 31$.

$$\gcd(6594, 2987) = \gcd(1099, 31).$$

6. *Prime check:* 31 is prime and does not divide 1099, so $\gcd(1099, 31) = 1$.

$$\boxed{\gcd(6594, 2987) = 1}$$

Comparison: 1 division with the tricks, against 7 in the plain Euclidean algorithm.

Example 15: $\gcd(1827, 8736)$

1. *Common factor:* $p = 3$ divides both, since the digit sum of 8736 is $8 + 7 + 3 + 6 = 24$ and the digit sum of 1827 is $1 + 8 + 2 + 7 = 18$. Hence $\gcd(ka, kb) = k \gcd(a, b)$ gives

$$\gcd(1827, 8736) = 3 \cdot \gcd(2912, 609).$$

2. *Remove a useless factor:* 2 divides 2912 (2912 ends in 2) but not 609 (609 ends in 9), so 2 cannot divide the gcd and we may cancel 2^5 from 2912: $2912 = 32 \cdot 91$.

$$\gcd(1827, 8736) = 3 \cdot \gcd(609, 91).$$

3. *Remove a useless factor:* 3 divides 609 (the digit sum of 609 is $6 + 0 + 9 = 15$) but not 91 (the digit sum of 91 is 10, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 609: $609 = 3 \cdot 203$.

$$\gcd(1827, 8736) = 3 \cdot \gcd(203, 91).$$

4. *Division:* $203 = 2 \cdot 91 + 21$, and $21 \leq 91/2$ is already the least absolute remainder.

$$\gcd(1827, 8736) = 3 \cdot \gcd(91, 21).$$

5. *Remove a useless factor:* 3 divides 21 (the digit sum of 21 is $2 + 1 = 3$) but not 91 (the digit sum of 91 is 10, not a multiple of 3), so 3 cannot divide the gcd and we may cancel it from 21: $21 = 3 \cdot 7$.

$$\gcd(1827, 8736) = 3 \cdot \gcd(91, 7).$$

6. *Divisibility check:* 7 divides 91 ($91 = 13 \cdot 7$), so $\gcd(91, 7) = 7$.

$$\gcd(1827, 8736) = 3 \cdot 7 = 21.$$

$$\boxed{\gcd(1827, 8736) = 21}$$

Comparison: 1 division with the tricks, against 8 in the plain Euclidean algorithm.
