The factor lemma

CJ Quines
April 12, 2025

Warmup

1. Let a, b, c, d, and p be positive integers.
   a) Prove that if $a \mid c$, $b \mid d$, and $p = ab$, then $p \mid cd$.
   b) Prove that if $p \mid cd$, then there exists a and b such that $a \mid c$, $b \mid d$, and $p = ab$.
2. (Baltic 1996/6) Let a, b, c, d be positive integers such that $ab = cd$. Prove that $a + b + c + d$ is not prime.
3. (Euclid's formula) Let a, b, c be positive integers such that $a^2 + b^2 = c^2$, $\gcd(a, b) = 1$, and a is odd. Prove that there exists integers u and v such that $\gcd(u, v) = 1$, $a = u^2 - v^2$, $b = 2uv$, and $c = u^2 + v^2$.

The factor lemma

From here, we use the (standard) notation $(a, b) = \gcd(a, b)$.

Lemma (Factor lemma)
Let a, b, c, d be positive integers such that $ab = cd$. Then there exists positive integers p, q, r, s such that

$$a = pq, \quad b = rs, \quad c = pr, \quad d = qs,$$

and $(q, r) = 1$.

Proof 1. Choose positive integers q and r such that $\frac{a}{c} = \frac{d}{b} = \frac{q}{r}$ and $(q, r) = 1$. Because $\frac{a}{c}$ in lowest terms is $\frac{q}{r}$, there's some positive integer p such that $a = pq$ and $c = pr$. Similarly, there's some positive integer s such that $d = qs$ and $b = rs$. □

Proof 2. As $a \mid cd$, there are positive integers p and q such that $p \mid c$, $q \mid d$, and $a = pq$. As $p \mid c$, there's a positive integer r such that $c = pr$; similarly there's a positive integer s such that $d = qs$. As $ab = cd$, we can solve for $b = rs$. □

Proof 3. We claim that $a = \dfrac{(a, c)(a, d)}{(a, b, c, d)}$. Indeed:

$$\begin{aligned}
(a, c)(a, d) &= (a^2, ac, ad, cd) && \text{(distributivity)} \\
&= (a^2, ac, ad, ab) && \text{(substitute } ab = cd\text{)} \\
&= a(a, b, c, d), && \text{(distributivity)}
\end{aligned}$$

as desired. We have similar equalities for b, c, and d. We can then choose:

$$p = (a, c), \quad q = \frac{(a, d)}{(a, b, c, d)}, \quad r = \frac{(b, c)}{(a, b, c, d)}, \quad s = (b, d).$$

□

Remarks

- It's also called the factoring lemma and (Euler's) four number theorem. Might as well prove it if you use it though.
- If $(a, b, c, d) = 1$, you also get $(p, s) = 1$.
- There are some generalizations I've never used, but it's an interesting exercise to prove them:
  - If $a, c \in \mathbb{R}$ and $b, d \in \mathbb{Z}$ such that $ab = cd$, then there exists $p \in \mathbb{R}$ and $q, r, s \in \mathbb{Z}$ such that $a = pq$, $b = rs$, $c = pr$, $d = qs$. (Induct on b.)
  - If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are integers such that $\prod a = \prod b$, then there exists integers $t_{i,j}$ such that $a_i = \prod_j t_{i,j}$ and $b_j = \prod_i t_{i,j}$. (Double induct.)

  These are both in Erdős and Surányi's *Topics in the Theory of Numbers*, which is a fun book.
- If these words make sense: the factor lemma holds for all UFDs, so it's true not only in $\mathbb{Z}$, but also $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$, $R[X]$ for any UFD R (and thus $R[X_1, \ldots, X_n]$).

Examples

1. (Baltic 1996/6) Let a, b, c, d be positive integers such that $ab = cd$. Prove that $a + b + c + d$ is not prime.

   Sketch 1: Write $d = \frac{ab}{c}$. Then

   $$a + b + c + d = \frac{ac + bc + c^2 + ab}{c} = \frac{(a + c)(b + c)}{c},$$

   which can't be prime.

   Sketch 2: Apply factor lemma and choose

   $$a = pq, \quad b = rs, \quad c = pr, \quad d = qs.$$

   Then $a + b + c + d = (p + s)(q + r)$, which can't be prime.

2. (Euclid's formula) Let a, b, c be positive integers such that $a^2 + b^2 = c^2$, $(a, b) = 1$, and a is odd. Prove that there exists integers u and v such that $(u, v) = 1$, $a = u^2 - v^2$, $b = 2uv$, and $c = u^2 + v^2$.

   Sketch: From $b^2 = (c - a)(c + a)$, apply factor lemma and choose

   $$b = pq = rs, \quad c - a = pr, \quad c + a = qs.$$

   From $pq = rs$, apply factor lemma again and choose

   $$p = wx, \quad q = yz, \quad r = wy, \quad s = xz.$$

   Then

   $$a = \frac{qs - pr}{2} = \frac{xyz^2 - w^2xy}{2} = \frac{xy}{2}\left(z^2 - w^2\right).$$

   Because a is odd, considering modulo 4 shows that $2 \mid xy$. We also get that $xy \mid 2a$. Combined with $xy \mid b$ and $(a, b) = 1$, we get that $xy = 2$. Thus $a = z^2 - w^2$, $b = 2zw$, and $c = z^2 + w^2$.

3. (Korea Final 2016/3) Prove that $x - \frac{1}{x} + y - \frac{1}{y} = 4$ has no solutions over the rationals.

   Sketch: Write $x = \frac{a}{b}, y = \frac{c}{d}$ in lowest terms. The given equation is
   $$a^2cb - b^2cd + abc^2 - abd^2 = 4abcd.$$
   Because a divides the RHS, it must divide the LHS, and thus $a \mid b^2cd$. But $(a, b) = 1$, so $a \mid cd$. Similarly, $b \mid cd$, $c \mid ab$, $d \mid ab$. Because $(a, b) = (c, d) = 1$, we get $ab \mid cd$ and $cd \mid ab$, so $ab = \pm cd$; for simplicity we consider only the positive case. Apply factor lemma and choose
   $$a = pq, \quad b = rs, \quad c = pr, \quad d = qs, \quad (q, r) = 1.$$
   The given equation becomes
   $$(p^2 - s^2)(q^2 + r^2) = 4pqrs.$$
   The RHS is 0 modulo 4. Because $(q, r) = 1$, $q^2 + r^2 \not\equiv 0 \pmod 4$. Thus $p^2 - s^2 \equiv 0 \pmod 4$, so $p \equiv s \pmod 2$. So in fact $p^2 - s^2 \equiv 0 \pmod 8$, and the RHS is also 0 modulo 8, so $2 \mid qr$. WLOG, q is even and r is odd. Via similar arguments with a, b, c, d, we get $4qr \mid p^2 - s^2$ and $ps \mid q^2 + r^2$, and these are in fact equalities. Now
   $$qr = \frac{p^2 - s^2}{4} = \left(\frac{p - s}{2}\right)\left(\frac{p + s}{2}\right),$$
   so setting $u = \frac{p-s}{2}$ and $v = \frac{p+s}{2}$, apply factor lemma on $qr = uv$ and set
   $$u = k\ell, \quad v = mn, \quad q = km, \quad r = \ell n, \quad (\ell, m) = 1.$$
   Then
   $$\begin{aligned} ps &= q^2 + r^2 \\ (k\ell + mn)(mn - k\ell) &= k^2m^2 + \ell^2n^2 \\ (m^2 - \ell^2)n^2 &= k^2(m^2 + \ell^2), \end{aligned}$$
   and because $(\ell, m) = 1$, we get $(m^2 - \ell^2, m^2 + \ell^2) = 1$, thus $k^2 = m^2 - \ell^2$ and $n^2 = m^2 + \ell^2$. We then get $n^4 - k^4 = (2\ell m)^2$, which has no solutions by Fermat's right triangle theorem.

Problems

These are mostly direct applications.

1. (ELMO 2009/1) Let a, b, c be positive integers such that $a^2 - bc$ is a square. Prove that $2a + b + c$ is not prime. **Hint:** 7

2. (Russia 2015/10/5) A square grid can be partitioned into n congruent tiles, each of size k. Prove that it is possible to partition it into k congruent tiles, each of size n. **Hint:** 4

3. (Moldova TST 2004/1) Suppose that a natural number n can be written as a sum of two squares of positive naturals in two different ways, in equations $n = a^2 + b^2 = c^2 + d^2$. Show that the number n is composite. **Hint:** 2

4. () Positive integers a, b, c, d satisfy $ab = cd$ and $a + b + c + d = (a - b)^2$. Prove that $4c + 1$ is a perfect square. **Hints:** 5 11

5. (IMO 2001/6) Let $a > b > c > d$ be positive integers and suppose that
   $$ac + bd = (b + d + a - c)(b + d - a + c).$$
   Prove that $ab + cd$ is not prime. **Hints:** 12 3

Other problems

These are less direct applications. Not necessarily harder than the last section.

6. (USA TSTST 2018/4(a)) For an integer $n > 0$, denote by $\mathcal{F}(n)$ the set of integers $m > 0$ for which the polynomial $p(x) = x^2 + mx + n$ has an integer root. Let S denote the set of integers $n > 0$ for which $\mathcal{F}(n)$ contains two consecutive integers. Show that S is infinite but

$$\sum_{n \in S} \frac{1}{n} \leq 1.$$

   Hints: 18 10

   Remark: Part (b) is: prove that there are infinitely many positive integers n such that $\mathcal{F}(n)$ contains three consecutive integers. But it's almost a different problem.

7. (USA TST 2021/1) Determine all integers $s \geq 4$ for which there exist positive integers a, b, c, d such that $s = a + b + c + d$ and s divides $abc + abd + acd + bcd$. **Hints:** 16 9

8. (IMO 1984/6) Let a, b, c, d be odd integers such that $0 < a < b < c < d$ and $ad = bc$. Prove that if $a + d = 2^k$ and $b + c = 2^m$ for some integers k and m, then $a = 1$. **Hints:** 17 14

9. (China TST 2006/7/3–) Find the largest positive integer M such that there exists integers a, b, c, d satisfying $ad = bc$ and $M \leq a < b \leq c < d \leq M + 49$. **Hints:** 19 1

10. (ISL 2018/N5) Four positive integers x, y, z and t satisfy the relations

$$xy - zt = x + y = z + t.$$

    Is it possible that both xy and zt are perfect squares? **Hints:** 21 8 15

11. (RMM 2023/1) Determine all prime numbers p and all positive integers x and y satisfying $x^3 + y^3 = p(xy + p)$. **Hints:** 6 20 13

Hints

1. The key claim is M works iff there's m, n such that $M \le mn$ and $(m+1)(n+1) \le M+49$.
2. Factor lemma, then solve for a, b in terms of p, q, r, s.
3. Apply the factor lemma to get p, q, r, s. Factor $3(ab+cd)$, and conclude.
4. Consider the area of the square.
5. Factor lemma, then set $m = p+s$, $n = q+r$. Take square roots.
6. Factor lemma to get a, b, c, d, such that $x+y = ab, x^2-xy+y^2 = cd, p = ac, xy+p = bd$. There's two cases. Show $a = p$ and $c = 1$ gives a contradiction, for size reasons.
7. Factor $a^2 - bc = n^2$.
8. Solve for x, y, a, and substitute into $xy = a^2$. Factor this as $(pqrs)^2 =$ (something)(something).
9. If s is prime, show that $ab \equiv cd \pmod{p}$. Do something similar to the first solution of Baltic 1996/6.
10. Show the sum is at most $\displaystyle\sum_{p,q>1} \frac{1}{p(p-1)q(q-1)}$.
11. Find a quadratic equation that has m/n as a rational root.
12. Manipulate to get $(a-b)$(something) $=(c+d)$(something).
13. Show $d < 3$ and $d > 3$ leads to no solutions, for size reasons. Conclude.
14. Do casework on each of the factors modulo 4.
15. Use size arguments on p, q, r, s and conclude.
16. If s is composite, pick a, b, c, d equal to pq, rs, pr, qs, then factor.
17. Factor lemma, then factor $a+b+c+d$ and $a-b-c+d$.
18. Use Vieta's to get an $ab = cd$ which you can factor lemma on.
19. Suppose M works. Use factor lemma to rewrite a and d, then relate to the inequalities.
20. When $a = 1$ and $c = p$, use $(x+y)^2 - 3xy = x^2 - xy + y^2$. Show $b \mid p$ leads to a contradiction, therefore $b \mid d-3$.
21. Let $xy = a^2$ and $zt = b^2$. Apply factor lemma on $(a-b)(a+b) = (z-x)(z-y)$.

Sketches

1. We have $a^2 - bc = n^2$ or $(a-n)(a+n) = bc$. Apply Baltic 1996/6 to get $(a-n)+(a+n)+b+c$ is not prime.

2. The area of the square is $s^2 = nk$. Apply factor lemma to choose $s = ab = cd$, $n = ac$, $k = bd$. Tile the square with $a \times c$ rectangles.

3. WLOG $a > c$, then $(a-c)(a+c) = (d-b)(d+b)$. Apply factor lemma to choose $a - c = pq$, $a + c = rs$, $d - b = pr$, $d + b = qs$. Then $a = \frac{pq+rs}{2}$, $b = \frac{qs-pr}{2}$, and $4n = (p^2+s^2)(q^2+r^2)$. If n was prime, then WLOG $n \mid q^2 + r^2$, and $p^2 + s^2$ is 2 or 4; both cases are impossible.

4. Apply factor lemma to choose $a = pq$, $b = rs$, $d = pr$, $c = qs$. Set $m = p + s$, $n = q + r$. The given equation becomes $mn = (qm - sn)^2$. Write $m = (m,n)m'^2$, $n = (m,n)n'^2$. Take square roots to get $\pm m'n' = qm'^2 - sn'^2$. Then $x = \frac{m'}{n'}$ is a rational root of the quadratic $qx^2 \mp x - s = 0$. Thus its discriminant $(\mp 1)^2 - 4q(-s) = 4c + 1$ is a perfect square.

5. Rearrange to get

$$\begin{aligned} ac + bd &= (b+d)^2 - (a-c)^2 \\ a^2 - b^2 - bd + ad &= d^2 - c^2 + ac + ad \\ (a-b)(a+b+d) &= (d+c)(d-c+a). \end{aligned}$$

   Apply factor lemma to choose $a - b = pq$, $a + b + d = rs$, $d + c = pr$, $d - c + a = qs$. Add everything to get $3(a+d) = pq + rs + pr + qs$. Solve for a, b, c, d:

$$\begin{aligned} 3a &= 2pq + 2rs - pr - qs, & 3b &= -pq + 2rs - pr - qs, \\ 3c &= pq + rs + pr - 2qs, & 3d &= -pq - rs + 2pr + 2qs. \end{aligned}$$

   Do more bashing to get

$$\begin{aligned} 3(ab + cd) &= -p^2q^2 + r^2s^2 + p^2r^2 - q^2s^2 + pq^2s - pr^2s \\ &= (r^2 - q^2)(p^2 + s^2 - ps). \end{aligned}$$

6. Say $x^2 + mx + n = (x+a)(x+b)$ and $x^2 + (m+1)x + n = (x+c)(x+d)$. Then $n = ab = cd$, and by factor lemma choose $a = pq$, $b = rs$, $c = pr$, $d = qs$. Also, $m + 1 = a + b + 1 = c + d$, so $(p-s)(q-r) = 1$. Both factors here must be 1, so $n = p(p-1)q(q-1)$. Then

$$\sum_{n \in S} \frac{1}{n} \le \sum_{p,\, q > 1} \frac{1}{p(p-1)q(q-1)} = \sum_{p>1} \left(\frac{1}{p-1} - \frac{1}{p} \right) \left(\sum_{q>1} \frac{1}{q-1} - \frac{1}{q} \right) = 1$$

   by telescoping.

7. It's all composite s. If s is composite, write $s = mn$. Set $(p,q,r,s) = (1, 1, m-1, n-1)$ and $a = pq$, $b = rs$, $c = pr$, $d = qs$. This works because $s = a + b + c + d = (p+s)(q+r) = mn$, and $\sum_{\text{cyc}} abc = ab(c+d) + cd(a+b) = pqrs(a+b+c+d)$ is divisible by $s = mn = pqrs$.

   If s is prime, then $a + b + c + d \equiv 0 \pmod{p}$, and $p \mid ab(c+d) + cd(a+b)$. And RHS here is $ab(-a-b) + cd(a+b) = (a+b)(cd - ab)$, so $ab \equiv cd \pmod{p}$. Again using a similar trick to Baltic 1996/6, write $d \equiv \frac{ab}{c} \pmod{p}$ and get $\frac{(a+c)(a+d)}{c} \equiv 0 \pmod{p}$, contradiction.

8. By factor lemma choose $a = pq$, $d = rs$, $b = pr$, $c = qs$; then $p < s$, $q < r$ and these are all odd. Also,

$$2^m(2^{k-m} + 1) = a + b + c + d = (s + p)(r + q),$$
$$2^m(2^{k-m} - 1) = a - b - c + d = (s - p)(r - q).$$

Now $s \pm p$ and $r \pm q$ are even, so we have four cases modulo 4:

- If $4 \mid s + p$ and $4 \mid r + q$, then $4 \nmid s - p$ and $4 \nmid r - q$, so $m = 2$, which is impossible for size reasons.
- Similarly, we can't have $4 \mid s - p$ and $4 \mid r - q$.
- If $4 \nmid s+p$ and $4 \nmid r-q$, then $2^{m-1} \mid s-p$ and $2^{m-1} \mid r+q$. Thus $2(s-p) \geq 2^m = pr+qs$, so $q = 1$; similarly $2(r + 1) \geq 2^m = pr + qs$, so $p = 1$, and $a = pq = 1$.
- Similarly, in the remaining case we also get $a = 1$.

9. We claim M works if there's m, n such that $M \leq mn$ and $(m + 1)(n + 1) \leq M + 49$.

($\Rightarrow$) Use factor lemma to choose $a = pq$, $d = rs$, $b = pr$, $c = qs$. Then $a < b$ means $q < r$, and $b < d$ means $p < s$. Then $M \leq a \leq pq \leq (s - 1)(r - 1)$, and we can take $m = s - 1$ and $n = r - 1$.

($\Leftarrow$) WLOG $m \leq n$, then take $(p, q, r, s) = (m, n, n + 1, m + 1)$ to get a, b, c, d.

By the claim, $m + n \leq 48$, and $M \leq mn \leq 24^2$, and indeed 24^2 works if we take $m = n = 24$.

10. No. FTSOC $xy = a^2$ and $zt = b^2$, and WLOG z is largest. Then $(a - b)(a + b) = xy - z(x + y - z) = (z - x)(z - y)$. Apply factor lemma to get $z - x = pq$, $z - y = rs$, $a - b = pr$, $a + b = qs$. Note that $x + y = a^2 - b^2 = pqrs$, so we can solve to get

$$2x = -pq + rs + pqrs, \quad 2y = pq - rs + pqrs, \quad 2a = pr + qs.$$

Substitute into $(2x)(2y) = (2a)^2$ to get $(pqrs)^2 = (p^2+s^2)(q^2+r^2)$. Now we do size arguments: by AM–GM the minimum is 1, so WLOG $p = 1$, and then we get $q^2r^2 \leq 2(q^2 + r^2)$, so $s = 1$ and $q = r = 2$, contradiction.

11. Apply factor lemma and write $x + y = ab$, $x^2 - xy + y^2 = cd$, $p = ac$, $xy + p = bd$. As p is prime, we have two cases.

If $a = p$ and $c = 1$, then $x^2 - xy + y^2 = d$ and $d \geq xy$ by AM–GM. Then $p \geq (b - 1)xy$, and $x + y \geq b(b - 1)xy$, which is impossible if $b > 1$ for size reasons. Thus $b = 1$, so $p = x + y$, and $p = (x - y)^2$, which is a contradiction.

Thus $a = 1$ and $c = p$. From $(x + y)^2 - 3xy = x^2 - xy + y^2$, we get $b^2 - 3bd = p(d - 3)$, and b divides the LHS, so it divides the RHS. If $b \mid p$, then from $xy + p = bd$ we get $p \mid xy$, contradiction. Thus $b \mid d - 3$. We have three cases. If $d < 3$, then $b = 2$, which leads to no solutions. If $d > 3$, then $d - 3 \geq b$ and $d > b = x + y$. But then

$$d = \frac{xy + p}{x + y} \leq \frac{xy + pd}{x + y} = \frac{x^2 + y^2}{x + y} \leq x + y = b,$$

contradiction. The remaining case is $d = 3$, whence $(x + y)^2 - 3xy = x^2 - xy + y^2$ becomes $b^2 - 9b + 3p = 3p$, and $b = 9$. Given that $(x, y) = 1$ and $x + y = b$, we can just check all possible x, y.