

15-251: Great Theoretical Ideas In Computer Science

Recitation 6 Solutions

Number Theory Statements

Below are some “if and only if” statements. Decide which directions (if any) of each statement are true. For implications that are true, give a short proof. For each that is false, give a counterexample. All letters below represent integer values.

1. n is odd if and only if $n^2 + 2n$ is odd.

Solution: Both implications are true. If n is odd, then n^2 is odd and $2n$ is even, so $n^2 + 2n$ is odd. On the other hand, if $n^2 + 2n = n(n+2)$ is odd, then both n and $n+2$ must be odd (since a divisor of an odd number is always odd).

2. $\gcd(x, y) = 1$ if and only if $\gcd(x^2, y^2) = 1$.

Solution: Both implications are true (just look at the prime factorizations).

3. $x|yz$ if and only if $x|y$ or $x|z$.

Solution: Only one direction is true: If $x|y$ then $x|yz$. Similarly, $x|z$ also implies $x|yz$. The other implication is false: it is possible for $x|yz$ but neither $x|y$ nor $x|z$. For example, let $x = 6$, $y = 3$ and $z = 4$. $6|(3)(4) = 12$ but 6 does not divide 3 or 4.

4. $x|(y + z)$ if and only if $x|y$ and $x|z$.

Solution: Again, one direction is true. For the other direction, $x = 2$ and $y = z = 1$ is a counterexample in that $x|(y + z)$ but x does not divide y or z .

5. $x|y$ if and only if $x^2|y^2$.

Solution: One implication is easily true: If $x|y$ then $x^2|y^2$. To see that the other implication is also true it is probably easiest to consider the prime factorizations of x^2 and y^2 . Formally, for each prime p and every positive integer z , let $v_p(z)$ denote the power of p in the prime factorization of z . Of course, $v_p(z^2) = 2v_p(z)$. Suppose that $x^2|y^2$. This just means that $v_p(x^2) \leq v_p(y^2)$ for each prime p . So $2v_p(x) \leq 2v_p(y)$ for every p and thus $v_p(x) \leq v_p(y)$ for every p which implies $x|y$.

6. $x|y$ if and only if $x^3|y^2$.

Solution: If $x|y$ then it is not always the case that $x^3|y^2$: $x = y = 2$ is an easy counterexample. On the other hand, the other direction is true. Indeed, if $x^3|y^2$, we may write $y^2 = dx^3$ for some integer d . Using associativity, we then have $y^2 = (dx)x^2$. But since the quantity on the left hand side is a perfect square, so must the quantity on the right hand side, which implies that dx is a perfect square, and so $j = \sqrt{dx}$ is an integer. Taking square roots, we have $y = \pm jx$, so $x|y$.

Modular Congruences

7. Find the smallest positive n such that $n \equiv 4482341 \pmod{11}$.

Solution: One simple way is to just divide 4482341 by 11: we get 6 as a remainder. Another slick way that avoids the explicit division is to note that

$$4482431 = 4 \cdot 10^6 + 4 \cdot 10^5 + 8 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 1 \cdot 10^0.$$

Now, as $10 \equiv -1 \pmod{11}$, this is

$$\begin{aligned} & 4 \cdot (-1)^6 + 4 \cdot (-1)^5 + 8 \cdot (-1)^4 + 2 \cdot (-1)^3 + 3 \cdot (-1)^2 + 4 \cdot (-1)^1 + 1 \cdot (-1)^0 \\ &= 4 - 4 + 8 - 2 + 3 - 4 + 1 \equiv 6 \pmod{11}. \end{aligned}$$

8. What is the units digit of 7^{7^7} ?

Solution: We notice first that when we take powers of seven, the first four powers (starting from 1) have units digits equal to 7, 9, 3, 1. This pattern then just repeats. Thus the question reduces to finding the units digit of $7^{7^7 \pmod{4}}$. Now to compute the exponent:

$$7^7 \equiv_4 3^7 \equiv_4 (-1)^7 \equiv_4 -1 \equiv_4 3$$

Thus the units digit of 7^{7^7} is the same as the units digit of $7^3 = 243$, which is 3. (Note that looking at the units digit is just working modulo 10.)

Euclid's Algorithm

9. Find all solutions to $17x + 47y = 4$.

Solution: Let us use Extended Euclid's algorithm to find values r, s such that $17r + 47s = 1$.

$$\begin{aligned} 47 &= 17 \times 2 + 13 \\ 17 &= 13 \times 1 + 4 \\ 13 &= 4 \times 3 + 1 \end{aligned}$$

Now we work backwards:

$$\begin{aligned} 1 &= 13 - 4 \times 3 \\ &= 13 - (17 - 13) \times 3 = 13 \times 4 - 17 \times 3 \\ &= (47 - 17 \times 2)4 - 17 \times 3 = 47 \times 4 - 17 \times 11 \end{aligned}$$

Hence $(-11) \cdot 17 + 4 \cdot 47 = 1$. Multiplying by 4, we get that some solution for $17x + 47y = 4$ is $x = -44, y = 16$. In general, for any integer z , $x = (-44 + 47z)$ and $y = (16 - 17z)$ is a solution.

Number Theory Proofs

10. Let d be any positive integer not equal to 2, 5, or 13. Show that you can find distinct (a, b) in the set $\{2, 5, 13, d\}$ such that $ab - 1$ is not a perfect square.

Solution: We will prove that one of $2d - 1$, $5d - 1$, and $13d - 1$ is not a perfect square. Suppose that all three were squares:

$$\begin{aligned} 2d - 1 &= x^2 \\ 5d - 1 &= y^2 \\ 13d - 1 &= z^2 \end{aligned}$$

We notice from the first equation that x is odd. Thus $x = 2k + 1$, and $x^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. Since either k is even or $k + 1$ is even, we have that $x^2 \equiv_8 1$. Applying our original equation for x^2 , we find:

$$2d \equiv_8 x^2 + 1 \equiv_8 2$$

which implies that d is odd. Then, both $5d$ and $13d$ are also odd, and we conclude that y and z are even. Let $y = 2u$ and $z = 2v$. We can then subtract $5d$ from $13d$ to get the following equation:

$$\begin{aligned} 8d &= (2u)^2 - (2v)^2 \\ \Rightarrow 2d &= u^2 - v^2 \\ \Rightarrow 2d &= (u+v)(u-v) \end{aligned}$$

Thus one of $u+v$ and $u-v$ must be even. But these must both have the same parity, and so they are both even. This implies that $4|2d$, so d must be even, which is a contradiction.

11. Prove that every year (including leap years) has at least one Friday the 13th.

Solution: We represent the days of the week as integers mod 7, with Sunday as 0, Monday as 1, etc. Then, if January 13th is on day x , we can compute what day the 13th of every other month falls on by looking at the previous month, and adding the number of days in that month mod 7. The following chart shows what day of the month the 13th lands on, for either a leap year or a non-leap year.

Month	Days in preceding month (mod 7)	Day of 13th (non-leap year)	Day of 13th (leap year)
1		x	x
2	3	$x+3$	$x+3$
3	0 (1 in leap year)	$x+3$	$x+4$
4	3	$x+6$	x
5	2	$x+1$	$x+2$
6	3	$x+4$	$x+5$
7	2	$x+6$	x
8	3	$x+2$	$x+3$
9	3	$x+5$	$x+6$
10	2	x	$x+1$
11	3	$x+3$	$x+4$
12	2	$x+5$	$x+6$

Both the leap year and non-leap year columns in this chart have entries congruent to every possible value mod 7. Therefore, no matter what the value of x , one of these must be a 6 (Friday).

More Fun With Phi

Recall from lecture that $\phi(n)$ is the number of positive integers less than or equal to n which are relatively prime to n .

12. Show that if $GCD(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$.

Solution: As in class, we will figure out how many numbers in \mathbb{Z}_{ab} share (non-trivial) factors with a , with b , and with both — and then we use inclusion-exclusion to count the number of elements in \mathbb{Z}_{ab}^* .

- Each number x in \mathbb{Z}_{ab} can be written in the form $Ba + A$, where $B \in \mathbb{Z}_b$ and $A \in \mathbb{Z}_a$ — B is the dividend and A is the remainder after dividing x by a . Ba always shares factors with a .

Therefore, whether x shares a factor with a is entirely determined by A —indeed, x shares a factor with a exactly when A shares a factor with a . Each such x then also shares a factor with ab . There are $a - \phi(a)$ choices for A such that A shares a factor with a . There are b choices for B (no restriction). Therefore, the number of such numbers x is $b(a - \phi(a))$.

- Similarly, each x can be written in the form $Ab + B$, and by a completely analogous argument, the number of x 's that share a factor with b (and therefore with ab) is $a(b - \phi(b))$.
- Finally, $(a - \phi(a))(b - \phi(b))$ numbers share factors with both a and b .

Therefore, the number of numbers that share factors with ab is

$$\begin{aligned} ab - \phi(ab) &= b(a - \phi(a)) + a(b - \phi(b)) - (a - \phi(a))(b - \phi(b)) \\ &= ab - b\phi(a) + ab - a\phi(b) - ab + b\phi(a) + a\phi(b) - \phi(a)\phi(b) \\ &= ab - \phi(a)\phi(b) \end{aligned}$$

So $\phi(ab) = \phi(a)\phi(b)$.

13. Show that if p is a prime number, then for all $k \geq 1$, $\phi(p^k) = p^{k-1}(p - 1)$.

Solution: The numbers from 1 to p^k that are *not* relatively prime to p^k are precisely the multiples of p in $p, 2p, \dots, (p^{k-1})p$. There are exactly $k - 1$ of these numbers. Thus, the number that *are* relatively prime to p^k is $p^k - p^{k-1} = p^{k-1}(p - 1)$.