Worksheet 4.3

Max's Lecture
MATH 55

July 5, 2019

Exercise A (from charles). 1. Express 74 in base 2. Express 27 in hexidecimal.

2. Convert the binary number 10101 to base 4. Do the same for base 8. Can you guess a pattern?

Did on previous work sheet.

Exercise B. Suppose that an integer is expressed in the standard decimal notation. How can you tell whether the number is divisible by 3? Why does your rule work?

Did on previous worksheet.

Exercise C. Determine whether 101 is a prime number.

We have a thm that says:

If n does not have prime divisor $\leq \sqrt{n}$, then n is prime.

If you check all the positive integers n s.t. $1 < n < \sqrt{101}$, so $n = 2, 3, 4, \ldots, 9, 10$,

you will see that none divide 101.

So 101 is prime.

Exercise D. Suppose you know the prime factorizations of two positive integers a and b. How can you find their gcd and their lcm. What is the product of $\gcd(a, b)$ and $\mathrm{lcm}(a, b)$?

Let $a = p_1^{s_1} \cdots p_n^{s_n}$ (where $p_1, \ldots, p_n$ is union of prime factors of a and b)

and

$b = p_1^{r_1} \cdots p_n^{r_n}$.

Then $\gcd(a,b) = p_1^{\min(s_1,r_1)} \cdots p_n^{\min(s_n,r_n)}$

and

$\mathrm{lcm}(a,b) = p_1^{\max(s_1,r_1)} \cdots p_n^{\max(s_n,r_n)}$

It turns out that $\gcd(a,b)\,\mathrm{lcm}(a,b) = ab$.

This is because for any integers x, y,

$\min(x,y) + \max(x,y) = x + y$.

Exercise E. Compute the gcd of 54 and 114 using the euclidean algorithm.

$114 = 2 \cdot 54 + \boxed{6}$

$54 = 6 \cdot 9 + 0$

So the gcd is 6

Exercise F. Use lemma 2 to prove the following, where a, b, c, m are positive integers and p is a prime:

1. If $p|ab$, then p must divide a or b.
2. If $ac \equiv bc(\mod m)$ and $\gcd(c, m) = 1$, then $a \equiv b(\mod m)$

Lemma 2 states that: If a, b, c are positive integers s.t. $\gcd(a,b) = 1$ and $a|bc$, then $a|c$.

1. Suppose for contradiction that $p|ab$ but p divides neither a nor b.

Since p is prime and p does not divide a, $\gcd(p, a) = 1$.

So by Lemma 2, p must divide b. This contradicts our assumption that p does not divide b.

So by contradiction the original statement holds.

2. Assume $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$. Since $ac \equiv bc \pmod m$, by definition, $m|ac - bc$. which we rewrite as $m|c(a-b)$.

Since c is relatively prime to m, by lema 2 we get that $m|(a-b)$ which means $a \equiv b \pmod m$ by definition.