

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Mathematics for Computer Science
MIT 6.042J/18.062J

Prime Factorization



Albert R Meyer

March 5, 2014

diehardprimes.1

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Fundamental Thm. of Arithmetic

Every integer > 1
factors **uniquely** into a
weakly decreasing
sequence of primes



Albert R Meyer

March 5, 2014

diehardprimes.2

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Unique Prime Factorization

Example:

$$61394323221 = 53 \cdot 37 \cdot 37 \cdot 37 \cdot 11 \cdot 11 \cdot 7 \cdot 3 \cdot 3 \cdot 3$$



Albert R Meyer

March 5, 2014

diehardprimes.3

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Prime Divisibility

Lemma: p prime and $p \mid ab$
implies $p \mid a$ or $p \mid b$

pf: say **not** $(p \mid a)$, so $\gcd(p, a) = 1$

so,
$$\underbrace{sa}_p b + \underbrace{tp}_p b = \underbrace{1}_p b$$

so $p \mid b$
QED



Albert R Meyer

March 5, 2014

diehardprimes.4

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Prime Divisibility

Cor : If p is prime, and
 $p | a_1 \cdot a_2 \cdots a_m$
 then $p | a_i$ for some i .
pf: by induction on m .



Albert R Meyer

March 5, 2014

diehardprimes.5

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Unique Prime Factorization

Every integer $n > 1$ has a
unique factorization into
 primes: $p_1 \cdots p_k = n$
 with $p_1 \geq p_2 \geq \cdots \geq p_k$



Albert R Meyer

March 5, 2014

diehardprimes.6

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Unique Prime Factorization

pf: suppose not. choose smallest $n > 1$:

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

$$p_1 \geq p_2 \geq \cdots \geq p_k$$

$$q_1 \geq q_2 \geq \cdots \geq q_m$$

If $q_1 = p_1$, then $p_2 \cdots p_k = q_2 \cdots q_m$
 is smaller nonunique.



Albert R Meyer

March 5, 2014

diehardprimes.7

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Unique Prime Factorization

pf: suppose not. choose smallest $n > 1$:

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

$$p_1 \geq p_2 \geq \cdots \geq p_k$$

$$q_1 \geq q_2 \geq \cdots \geq q_m$$

So can assume $q_1 > p_1 \geq p_i$



Albert R Meyer

March 5, 2014

diehardprimes.8

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Unique Prime Factorization

pf: but $q_1 | n = p_1 \cdot p_2 \cdots p_k$
so $q_1 | p_i$ for some i by Cor,
contradicting that $q_1 > p_i$
QED

