2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

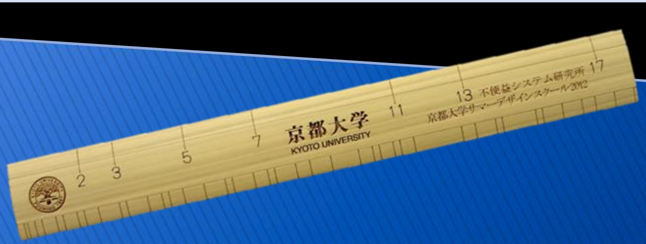
More Fun with Prime Numbers

Week 1

What are Prime Numbers?

Tetsushi Ito

Department of Mathematics
Kyoto University



Infinitude of Prime Numbers (1)

Definition

An integer N ≥ 2 is a **prime number** if it is divisible only by 1 and itself.

Examples

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ⋯

- Many interesting properties, deep theorems, conjectures, and open (unsolved) problems.

Infinitude of Prime Numbers (2)

- This course
  - Basics on Prime Numbers (Week 1)
  - Laws of Prime Numbers (Week 2, 3)
  - Applications to Cryptography (Week 4)
  - Recent Developments/Open Problems (Week 5)
- Let’s become a **Master of Prime Numbers!**

Infinitude of Prime Numbers (3)

Theorem (**Prime Factorization**)
Every $N \geq 1$ can be written as a product of prime numbers

$$N = P_1 \times P_2 \times \cdots \times P_r$$

and the prime numbers $P_1, P_2, \cdots, P_r$ are **unique up to permutation**.

Example

$$36 = 2 \times 2 \times 3 \times 3 = 2 \times 3 \times 2 \times 3$$

- Prime Numbers ≒ Atoms of numbers

Infinitude of Prime Numbers (4)

Theorem (Euclid)
There are **infinitely many** prime numbers.

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73
79 83 89 97 101 103 107 109 113 127 131 137 139 149 151
157 163 167 173 179 181 191 193 197 199 211 223 227 229
233 239 241 251 257 263 269 271 277 281 283 293 307 311
313 317 331 337 347 349 353 359 367 373 379 383 389 397
401 409 419 421 431 433 439 443 449 457 461 463 467 479
487 491 499 503 509 521 523 541 547 557 563 569 571 577
587 593 599 601 607 613 617 619 631 641 643 647 653 659
661 673 677 683 691 701 709 719 727 733 739 743 751 757
761 769 773 787 797 809 811 821 823 827 829 839 853 857
859 863 877 881 883 887 907 911 919 929 937 941 947 953
967 971 977 983 991 997....... (**infinitely many**)

Euclid of
Alexandria
(fl. 300BC)

https://en.wikipedia.org/wiki/Euclid

Infinitude of Prime Numbers (5)

Euclid's proof

Let $P_1, P_2, \cdots, P_r$ be a given set of prime numbers. We shall show there is a prime number outside this set. Put

$$M = P_1 \times P_2 \times \cdots \times P_r + 1.$$

By **Unique Factorization**

$$M = Q_1 \times Q_2 \times \cdots \times Q_s.$$

Then Q_1 is different from $P_1, P_2, \cdots, P_r$ because M is divisible by Q_1, but **not** by $P_1, P_2, \cdots, P_r$.

Interlude: Grothendieck’s Prime

Alexander
Grothendieck
(1928-2014)

57 is **Grothendieck’s Prime**.

(But···, $57 = 3 \times 19$)

https://en.wikipedia.org/wiki/Alexander_Grothendieck