A BRIEF PRIME CURIOS! GLOSSARY

CHRIS K. CALDWELL AND G. L. HONAKER, JR.

This brief glossary is written to explain some of the definitions we use at the Prime Curios! website: `http://primes.utm.edu/curios/`. A term used only once or twice can be defined in the curio itself, so those we have here are for terms that are used repeatedly. Please let us know of any errors or missing terms.

TABLE 1. Symbols and Other Notations

symbol	name	example
p_i	the i^{th} prime	$p_7 = 17$
$\pi(x)$	prime counting function	$\pi(100) = 25$
$n!$	n factorial	$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$
F_n	Fermat number $2^{2^n} + 1$	$F_3 = 2^8 + 1 = 257$
$fib(n)$	Fibonacci number	$fib(n+1) = fin(n) + fib(n-1)$
$M(n)$	Mersenne number $2^n - 1$	$M(7) = 2^7 - 1 = 127$
$n!_j$	n multifactorial	$10!_3 = 10 \cdot 7 \cdot 4 \cdot 1$
$n\#$	n primorial (prime-factorial)	$10\# = 7\# = 7 \cdot 5 \cdot 3 \cdot 2$
digit_i	subscript (repetition) operator	$1_2(34)_5 = 113434343434$

absolute prime: a prime that remains prime for all permutations of its digits. E.g., 199, 919 and 991 are all prime. Goal: definitions balanced with curio info.

almost-all-even-digits prime: a prime with all even digits except for one odd right-most digit. E.g., $666 \cdot 10^{14020} + 1$.

almost-equi-pandigital prime: a prime with all digits equal in number, except for one particular digit. E.g., $(1098765432123456789 0)_{42}1$.

alternate-digit prime: a prime that has alternating odd and even digits such as $(1676)_{948}1$.

beastly prime: a palindromic prime with 666 in the center, 0's surrounding these digits, and 1 or 7 at the end. Note that a non-palindromic beastly prime begins with a 666, followed by 0's, with either a 1 or 7 at the right end. E.g., $(10^{2475} + 666) \cdot 10^{2473} + 1$.

bemirp: (or bi-directional emirp) a prime that yields a different prime when turned upside down with reversals of both being two more different primes. E.g., 1061.

Date: September 14, 2006 (draft).

Bertrand's Postulate: In 1845 Bertrand postulated that if $n > 3$, then there is at least one prime between n and $2n - 2$. This was proven by Chebyshev in 1850.

ceiling function: denoted $\lceil x \rceil$, the least integer greater than or equal to x. $\lceil \pi \rceil = 4$, $\lceil -\pi \rceil = -3$, and $\lceil n \rceil = n$ for any integer n. The floor and ceiling functions were introduced by K. E. Iverson in 1962.

certificate of primality: a succinct summary of the proof that the given number is prime which contains just enough information to reproduce the proof.

Chen prime: a prime number p is called a Chen prime if $p + 2$ is either a prime or a semiprime. Chen Jingrun proved that there are infinitely many such primes.

circular prime: a prime that remains prime when we "rotate" its digits (e.g., 1193, 1931, 9311 and 3119 are prime). The known examples are 2, 3, 5, 7, 11, 13, 17, 37, 79, 113, 197, 199, 337, 1193, 3779, 11939, 19937, 193939, 199933 and, of course, the repunit primes.

composite: an integer greater than one which is not prime. Note that 1 is a unit, so is neither prime nor composite.

composite digit prime: a prime that has only the digits 4, 6, 8, or 9. E.g., $9 \cdot 10^{48051} - 1$.

coprime: the integers a and b are said to be coprime (or relatively prime) if they have no common factor other than 1 or -1, or equivalently, if their greatest common divisor is 1.

cousin primes: a pair of prime numbers that differ by four, e.g., 3 and 7. There should be infinitely many of these.

cryptology: the science of making and breaking secure codes. It consists of cryptography, the science of making secure codes, and cryptanalysis, the science of breaking them.

cuban primes: have the form $(n + 1)^3 - n^3$. The first few are 7, 19, 37, 61, 127, 271, ...

Cullen prime: primes of the form $n \cdot 2^n + 1$ (the only known examples are $n = 1$, 141, 4713, 5795, 6611, 18496, 32292, 32469, 59656, 90825, 262419, 361275, and 481899). Named after Reverend J. Cullen who published a question about them in 1905.

deletable prime: a prime in which you can delete the digits one at a time in some order and get a prime at each step. Defined by Caldwell in 1987, a deletable prime year.

depression prime: a palindromic prime having a repeating interior digit and two equal, but larger, end digits. E.g., 101, 757 and $72_{723}7$.

Dirichlet's theorem on primes in arithmetic progressions: if a and b are relatively prime, then there are infinitely many primes of the form $an + b$. E.g., there are infinitely many primes of the forms $3n + 1$ and $7n - 2$.

divisor: an integer d divides n if there is another integer q so that $dq = n$. In this case d is called a divisor (and a factor) of n and we denote this as $d|n$. Often the word is restricted to positive divisors, so the divisors of 6 are 1, 2, 3 and 6.

ECPP: (acronym for Elliptic Curve Primality Proving) a class of algorithms that provide certificates of primality using sophisticated results from the theory of elliptic curves. In practice, it is the fastest general-purpose primality-testing algorithm.

economical number: one for which the factorization requires fewer digits that the original number such as $256 = 2^8$ (compare to extravagant number).

emirp: a prime that gives a different prime when you reverse its digits (compare to palindromic prime). E.g., 389 and 983.

equidigital number: one for which the factorization requires the same number of digits as the original number. This includes all prime numbers.

Euler zeta function: the following sum (defined for $\Re(s) > 1$) and equivalent product:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots = \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdots$$

executable prime: a prime such that if stored on the proper computer hardware (in binary) is an executable program. E.g., $38 * 256 + 195$ is ES:RET (segment override) on an X86 system. Introduced by Carmody and Caldwell on September 11, 2001.

extravagant number: one for which the factorization requires more digits that the original number such as $30 = 2 \cdot 3 \cdot 5$ (compare to economical number).

factor: see divisor.

factorial primes: are primes of the form $n! \pm 1$. There are probably infinitely many, but only a few dozen are known.

Fermat number: a number of the form $2^{2^n} + 1$. Fermat knew these are prime for $n = 0$, 1, 2, 3, and 4; but it now seems likely that all of the rest are composite.

Fermat prime: Fermat numbers which are prime. Named after Fermat from a letter he wrote Mersenne on December 25, 1640.

Fermat's little theorem: states that if p is prime, then p divides $a^p - a$ for all integers a. When p does not divide a, this is sometimes written as $a^{p-1} \equiv 1 \pmod{p}$.

Fibonacci number: the numbers in the sequence 1, 1, 2, 3, 5, 8, 13, 21, ... where each is the sum of the proceeding two (often denoted u_1, u_2, u_3 ...). From the text *Liber Abaci* written by Fibonacci in 1202.

Fibonacci prime: a prime Fibonacci number. These will be numbers u_p where p is prime.

floor function $\lfloor x \rfloor$: the greatest integer less than or equal to x. E.g., $\lfloor 5.8n \rfloor$ is prime for $n = 1, 2, \ldots, 6$.

Fortunate number: Let P be the product of the first n primes and let q be the least prime greater than P. The nth Fortunate number is $q - P$. The sequence begins 3, 5, 7, 13, 23, 17, 19, 23, 37, 61, 67, 61, 71 ... These were conjectured to be all prime by Reo Fortune (once married to the famed anthropologist Margaret Mead).

Gaussian Mersenne prime: primes $2^n - (-1)^{(n^2-1)/8} 2^{(n+1)/2} + 1$ which are the norms of the Gaussian integers $(1 \pm i)^n - 1$. Prime for $n = 2$, 3, 5, 7, 11, 19, 29, 47, 73, 79, 113, 151, 157, 163, 167, 239, 241, 283, 353 ...

generalized Cullen prime: any prime that can be written in the form $n \cdot b^n + 1$ with $n + 2 > b$. E.g., $669 \cdot 2^{128454} + 1 = 42816 \cdot 8^{42816} + 1$.

generalized Fermat prime: primes $F_{b,n} = b^{2^n} + 1$ for an integer b greater than one.

generalized repunit: primes that are repunits in radix (base) b, i.e., $(b^n - 1)/(b - 1)$. Mersenne primes are generalized repunits in binary.

gigantic prime: one with at least $10,000$ digits.

GIMPS: (an acronym for the Great Internet Mersenne Prime Search) a collaborative project seeking Mersenne primes (see www.mersenne.org).

good prime: A prime p_i is called "good" if $p_i^2 > p_{n-i}p_{n+i}$ for $1 \leq i < n$. The first few are 5, 11, 17, 29, 37, 41, 53, 59, and 67.

high jumpers: a jumping champion (see jumping champion).

holey primes: are primes that have only digits with holes, i.e., 0, 4, 6, 8, or 9. E.g., 4649 and $9_{593}400049_{593}$.

Honaker's problem: asks for all consecutive prime number triples $p < q < r$ where p divides $qr + 1$. It is likely that the only such triplets are $(2, 3, 5)$, $(3, 5, 7)$, and $(61, 67, 71)$.

iccanobiF prime: a prime that becomes a Fibonacci number when reversed. E.g., 52057

illegal prime: a prime which represents information forbidden by law to possess or distribute. A prime found by Phil Carmody when written as a binary string was a computer program which bypasses copyright protection schemes on some DVDs. It was illegal at the time it was found.

integer: the positive natural numbers: 1, 2, 3, ...; their negatives: -1, -2, -3, ...; and zero.

invertible prime: a prime which yields a different prime when the digits are inverted. Must contain only the digits 0, 1, 3, 6, and 9.

irregular prime: see regular prime.

jumping champion: an integer n is jumping champion if n is the most frequently occurring difference between consecutive primes less than x, for some x. For $x = 3$ the jumping champion is 1; for $7 < x < 100$ it is 2; for $131 < x < 138$ it is 4; and for $389 < x < 420$ it is 6.

k-tuple: a repeatable pattern of primes that are as close as possible together. For example, twin primes are 2-tuples.

left-truncatable prime: are numbers that remain prime no matter how many of the leading digits are omitted.

Lucas number: the numbers in the Fibonacci-like sequence 2, 1, 3, 4, 7, 11, ...

Lucas prime: a prime Lucas number.

mega prime: those with one-million or more digits.

Mersenne numbers: are integers of the form $M_n = 2^n - 1$.

Mersenne prime: a prime Mersenne number $M_p = 2^p - 1$. Euclid mentioned these in his ancient geometry text *The Elements*. Some two-thousand years later they were named after Mersenne when he wrote about them to others in 1644.

Mills' prime: in 1947 Mills' proved there was a constant A such that $\lfloor A^{3^n} \rfloor$ is prime for all n. The primes that the smallest choice of A gives are the Mills' primes.

minimal prime: every prime, when written in base ten, has one of the 26 minimal primes as a substring: 2, 3, 5, 7, 11, 19, 41, 61, 89, 409, 449, 499, 881, 991, 6469, 6949, 9001, 9049, 9649, 9949, 60649, 666649, 946669, 60000049, 66000049, 66600049.

multifactorial prime: $n!_k = n(n-k)(n-2k) \cdot \ldots \cdot m$ (where m is between 1 and k). Primes $n!_k \pm 1$ are multifactorial primes.

naughty (or naughtiest) prime: a prime that is composed of mostly naughts (that is, zeros). E.g., 1000000007, $10^{24} + 7$ and $10^{60} + 7$.

near-repdigit prime: a prime with all like or repeated digits but one. E.g., 31, 331, 3331 and 33331.

near-repunit prime: a prime all but one of whose digits are 1. E.g., 71111111, 11111111113, and 2111111111111.

new Mersenne conjecture: (or Bateman, Selfridge, and Wagstaff conjecture) states that for any odd natural number p, if any two of the following conditions hold, then so does the third: (i) $p = 2^k \pm 1$ or $p = 4^k \pm 3$ for some natural number k. (ii) $2^k \pm 1$ is a (Mersenne) prime. (iii) $(2^p + 1)/3$ is a(Wagstaff) prime. The conjecture can be thought of as an attempt to salvage the centuries old "Mersenne conjecture," which is false

NSW prime: primes $((1 + \sqrt{2})^{2m+1} + (1 - \sqrt{2})^{2m+1})/2$ named after Newman, Shanks, and Williams (not New South Wales!)

number theory: (or higher arithmetic) the study of the properties of integers. Sometimes called the Queen of Mathematics.

ordinary prime: a prime p for which none of $p^n \pm 1$ (for small n) factor enough to make the number easily provable.

pandigital prime: a prime with all 10 digits, i.e., $0 - 9$. The first few are 10123457689, 10123465789, and 10123465897.

palindrome: (from the Greek palindromos "running back again") is a word, verse, sentence, or integer that reads the same forward or backward. E.g., "able was I ere I saw Elba" or 333313333.

palprime: (or palindromic prime) a prime that is a palindrome (such as 133020331).

perfect numbers: those that equal the sum of their proper divisors. Even perfect numbers, like 6 and 28, are a product of a Mersenne prime and a power of two. No odd perfect numbers are known.

period: (of a decimal expansion) the length of the repeating part (if any) of the decimal expansion. E.g., $1/7 = 0.14285714285714\ldots$ has period 6.

Pierpont prime: a prime greater than 3 having the form $2^u 3^v + 1$. These start 2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, ...

plateau prime: a palindromic prime having all equal internal digits and matching smaller end digits. E.g., 1777771, 355555553, and $5 * (10^{141} - 1)/9 - 2 * (10^{140} + 1)$.

prime counting function: $\pi(x)$ is the number of primes less than or equal to x. E.g., $\pi(3.14) = 2$ and for large x, $\pi(x)$ is approximately $x/\log x$.

prime curiologist: a person obsessed with "prime curios" (perhaps you?)

prime number: integer *greater than one* whose only positive divisors (factors) are 1 and itself. 1 is neither prime nor composite, it is an identity and a unit.

prime number theorem: (or PNT) this theorem states that the number of primes less than or equal to x, is about $x/\log x$; so the primes "thin out" as one looks at larger and larger numbers.

primeval number: a prime which "contains" more primes in it than any preceding number. Here "contains" means may be constructed from a subset of its digits. E.g., 1379 contains

3, 7, 13, 17, 19, 31, 37, 71, 73, 79, 97, 137, 139, 173, 179, 193, 197, 317, 379, 397, 719, 739, 937, 971, 1973, 3719, 3917, 7193, 9137, 9173, and 9371.

proper divisor: (or aliquot divisor) any positive divisor of n other than n itself. E.g., the proper divisors of 6 are 1, 2, and 3.

n-primorial denoted $n\#$: the product of the primes less than or equal to n. $6\# = 5\# = 5 \cdot 3 \cdot 2 = 30$. This notation was introduced by Harvey Dubner.

primorial prime: a prime of the form $n\# + 1$ or $n\# - 1$. Those with $n < 1000$ are $2\# + 1$, $3\# + 1$, $5\# + 1$, $7\# + 1$, $11\# + 1$, $31\# + 1$, $379\# + 1$; and $3\# + 1$, $5\# + 1$, $11\# + 1$, $13\# + 1$, $41\# + 1$, $89\# + 1$, $317\# + 1$, $337\# + 1$, $991\# + 1$.

probable prime: Numbers which pass tests that all primes pass, but few composites do, are called probable primes. E.g., the base a Fermat probable primes (a-PRPs) are those n which divide $a^{n-1} - 1$.

Proth prime: primes of the form $k \cdot 2^n + 1$ with $2^n > k$. These are named after the self-taught farmer François Proth who lived near Verdun, France (1852-1879) and published a theorem for proving their primality.

public-key cryptography: a type of cryptography in which the encoding key is revealed without compromising the encoded message. E.g., the RSA algorithm.

pseudoprime: a composite probable prime. At one time all probable primes were called pseudoprimes, but now this term is limited to composites.

regular prime: an odd prime number p is regular if it does not divide the class number of the p-th cyclotomic field; otherwise it is irregular.

repunit prime: a prime whose digits are all 1's: $R_n = (10^n - 1)/9$. E.g., 11, 1111111111111111 and 11111111111111111111.

Riemann hypothesis: states that the real part of any non-trivial zero (solution) of the Riemann zeta function is 1/2. It has remained unproven ever since its formulation by Bernhard Riemann in 1859, and is central to understanding the general distribution of primes. A $1,000,000 prize has been offered by the Clay Mathematics Institute for a proof.

Riemann zeta function: Riemann extended Euler's zeta function to one defined for all complex numbers except 1, and which obeys the functional equation:

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

right-truncatable primes: remain prime even if you stop before writing all of the digits e.g., 73939133). Also known as **snowball primes**.

RSA algorithm: perhaps the most famous of all public-key cryptosystems. Ronald Rivest, Adi Shamir, and Leonard Adleman at MIT announced it in 1977. It relies on the relative ease of finding large primes and the comparative difficulty of factoring integers for its security.

RSA numbers: are composite numbers having exactly two prime factors (semiprimes) that have been listed in the Factoring Challenge of RSA Security ®.

safe prime: a prime p for which $(p - 1)/2$ is also prime. These are "safer" when used in certain types of encryption.

self-descriptive primes: describe themselves as the digits are read. E.g. 10153331 reads "One 0, one 5, three 3's and three 1's."

semiprime: is the product of two primes, which is sometimes called a $P2$ or a 2-almost prime. The largest known semiprime is always the square of the largest known prime.

sexy primes: pairs of prime numbers that differ by six. Note that *sex* is Latin for six.

Smarandache-Wellin prime: a prime that is the concatenation of the first n prime numbers. E.g., 2, 23, 2357, and the concatenation of the first 128 primes.

snowball primes: see right-truncatable.

Sophie Germain prime: primes p for which $2p + 1$ is also prime (compare to safe primes). In about 1825 she proved the first case of Fermat's last theorem for exponents divisible by such primes.

strobogrammatic: primes are primes which remain the same number when rotated 180 degrees (e.g., 619). These may only have the digits 0, 1, 6, 8 and 9.

tetradic: primes, like 18181, remain the same viewed forward and backwards, while upside-right or upside-down. Such numbers may only have the digits 0, 1, and 8.

titanic: primes are those with 1000 or more decimal digits. In the mid-80s, Samuel Yates coined the name and called those who proved their primality, "titans."

triadic: (or 3-way) prime is one which is invariant upon reflection only across the line they are written on, so the digits may be 0, 1, 3, and 8. Trigg called these **palindromic reflectable**.

triplet: a prime triplet is three consecutive primes such that the first and the last differ by six. E.g., $(11, 13, 17)$. There should be an infinite number of these.

truncatable: prime numbers (without the digit zero) that remain prime no matter how many of the leading digits are omitted. E.g., 4632647 is left-truncatable because it and each of its truncations: 632647, 32647, 2647, 647, 47, and 7, are prime. Compare with left-truncatable.

twin prime: pairs of primes p and $p + 2$. It is conjectured that there are infinitely many of these.

unholey prime: a prime that does not have any digits with holes in them (see holey primes).

unique prime: (or unique period prime) a prime p which has a period (i.e., the decimal expansion of $1/p$ repeats in blocks of some set length) that it shares with no other prime. The period of a prime p always divides $p - 1$.

Vinogradov's theorem: states that every sufficiently large odd number is a sum of 3 primes. It is closely related to both Goldbach's and Waring's prime number conjectures.

Wagstaff prime: a prime of the form $(2^p + 1)/3$. These appear in the New Mersenne Conjecture and have applications in cryptography.

Wall-Sun-Sun prime: a prime $p > 5$ such that p^2 divides the Fibonacci number $u_{p-(p|5)}$ where $(p|5)$ is the Legendre symbol. None are known!

Wieferich prime: a prime p such that p^2 divides $2^{p-1} - 1$. Note that 1093 and 3511 are the only known such primes. All primes p divide $2^{p-1} - 1$.

Wilson prime: a prime p such that p^2 divides $(p - 1)! + 1$. The only known Wilson primes are 5, 13, and 563; there are no others less than $500,000,000$. All primes p divide $(p - 1)! + 1$.

Wolstenholme primes: primes p which divide B_{p-3}, where B_n is the nth Bernoulli number. After searching through all primes up to $500,000,000$, the only known Wolstenholme primes remains the lonely pair 16843 and 2124679.

Woodall primes: primes of the form $n \cdot 2^n - 1$. The Woodall primes are sometimes called the **Cullen primes of the second kind**.

Yarborough prime: a prime that does not contain the digits 0 or 1. An anti-Yarborough prime contains only 1's and 0's.

Zeta function: see the Euler zeta function and Riemann zeta functions.

University of Tennessee at Martin, Martin, TN 38238
E-mail address: caldwell@utm.edu

Bristol Virginia Public Schools, Bristol, VA 24201
E-mail address: honak3r@bvunet.net