信息安全数学基础

第一章 整除

熊虎
电子科技大学

第一章 整数

1.3素数、算数基本定理

定义1.3.1（素数） n是一个整数，且$n \neq 0, n \neq \pm 1$，若n只有平凡因数，则称整数n为素数，否则称为合数。

定理1.3.1 设p是一个素数，a, b 为任意整数。

（1）若$p \nmid a$，则p与a 互素；

证明： 设$\gcd(p, a) = d$，则有$d|p, d|a$。因为p是素数，所有由$d|p$可得$d = p$或$d = 1$。对于 $d = p$，由 $d|a$ 可得 $p|a$，与$p \nmid a$矛盾。因此，$d = 1$，即p与a互素。

1.3素数、算数基本定理

（2）若 $p|ab$ ，则 $p|a$ 或 $p|b$ 。一般地若 $p|a_1, a_2, \cdots a_k$ ，则必然存在某个 i ，$p|a_i$ 成立。

证明： 若 $p|a$ 则定理成立。若 $p \nmid a$ 成立，则 p 与 a 互素，由1.2节推论1.2.1可知 $p|b$ 。对于一般情形可以类推。

定理1.3.2（算术基本定理）

任一不为1的非零正整数 n 均可唯一地表示为

可利用如下递推公式得到：

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

其中，$p_1 < p_2 < \ldots < p_k, \alpha_1, \alpha_2, \ldots, \alpha_k$ 是正整数。

上式称为n的标准分解式。

1.3素数、算数基本定理

证明：（存在性）若n是素数，定理显然成立。

若n不是素数，设p_1是n的最小非平凡正因数，则p_1是素数，因为p_1的非平凡正因数也是n的非平凡正因数，所以p_1没有非平凡正因数。设$n=p_1n_1(1<n_1<n)$。对n_1重复上述推理，可得$n=p_1n_1=p_1p_2n_2$（p_2是素数，$1<n_2<n_1$）。以此类推，得$n>n_1>n_2>\cdots>1$，其步骤不超过n，最后必有$n=p_1p_2\cdots p_l$。

将上式中相同素数合并为素数的方幂，并按定理要求排列，就得到了分解的存在性。

1.3素数、算数基本定理

（惟一性）设n可分解为 $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}=q_1^{\beta_1}q_2^{\beta_2}\cdots q_l^{\beta_l}$
其中$p_1<p_2<...<p_k, q_1<q_2<...<q_l$都是素数。

根据定理1.3.1，存在某个 q_i 满足 $p_1|q_i$ ，不妨设为q_1，因为 p_1 和q_1都为素数，所以 $p_1=q_1$ 。类似地，可依次得到

$$p_i=q_i, 2\le i\le k$$

因此有$k=l$。又若$\alpha_1>\beta_1$ 则

$$p_1^{\alpha_1-\beta_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}=p_2^{\beta_2}\cdots p_k^{\beta_k}$$

上式左边被p_1整除，右边不能被p_1整除，矛盾，所以 $\alpha_1>\beta_1$ 不成立。同理 $\alpha_1<\beta_1$ 也不成立。故 $\alpha_1=\beta_1$ 。类似可证明 $\alpha_i=\beta_i(2\le i\le k)$

定理得证。

1.3素数、算数基本定理

定理1.3.3 素数有无穷多个。

证 反证法。假设只有有限个素数，设为：$p_1, p_2, \cdots, p_k$,令

$$M = p_1 p_2 \cdots p_k + 1$$

任何一个 $p_i, 1 \leq i \leq k$，都不整除 M，所以它们都不是M的素因子。由算术基本定理，M总有一个素因子，记为p，则$p \neq p_i, 1 \leq i \leq k$，与假设矛盾。因此素数有无限多个。

1.3素数、算数基本定理

Eratosthenes筛法

定理1.3.4 设n是一个正合数，p是n的大于1的最小正因数，则p是素数且$p \le \sqrt{n}$。

证明： 由定理1.3.2的证明过程可知，p是素数。
因为n是合数，所以存在整数n_1使得

$$n = pn_1, 1 < p \le n_1 < n$$

所以有$p^2 \le n$，即$p \le \sqrt{n}$。

1.3素数、算数基本定理

定理1.3.5 设n是一个正整数。如果对于所有的素数$p \le \sqrt{n}$，都有 $p \nmid n$ ，则 n是素数。

例1.3.1 求出100以内的所有素数。

解 小于等于$\sqrt{100}$ 的所有素数：2，3，5，7，其倍数：

$$
\begin{array}{lllll}
2\cdot 2, & 3\cdot 2, & 4\cdot 2, & \ldots, & 49\cdot 2, \quad 50\cdot 2 \\
2\cdot 3, & 3\cdot 3, & 4\cdot 3, & \ldots, & 32\cdot 3, \quad 33\cdot 3 \\
2\cdot 5, & 3\cdot 5, & 4\cdot 5, & \ldots, & 19\cdot 5, \quad 20\cdot 5 \\
2\cdot 7, & 3\cdot 7, & 4\cdot 7, & \ldots, & 13\cdot 7, \quad 14\cdot 7.
\end{array}
$$

1.3素数、算数基本定理

对于素数 $p_1 = 2$,

1	2	3	$\not 4$	5	$\not 6$	7	$\not 8$	9	$\not 10$
11	$\not 12$	13	$\not 14$	15	$\not 16$	17	$\not 18$	19	$\not 20$
21	$\not 22$	23	$\not 24$	25	$\not 26$	27	$\not 28$	29	$\not 30$
31	$\not 32$	33	$\not 34$	35	$\not 36$	37	$\not 38$	39	$\not 40$
41	$\not 42$	43	$\not 44$	45	$\not 46$	47	$\not 48$	49	$\not 50$
51	$\not 52$	53	$\not 54$	55	$\not 56$	57	$\not 58$	59	$\not 60$
61	$\not 62$	63	$\not 64$	65	$\not 66$	67	$\not 68$	69	$\not 70$
71	$\not 72$	73	$\not 74$	75	$\not 76$	77	$\not 78$	79	$\not 80$
81	$\not 82$	83	$\not 84$	85	$\not 86$	87	$\not 88$	89	$\not 90$
91	$\not 92$	93	$\not 94$	95	$\not 96$	97	$\not 98$	99	$\not 100$

对于素数 $p_2 = 3$,

1	2	3	5	7	$\not 9$
11		13	$\not 15$	17	19
$\not 21$		23	25	$\not 27$	29
31		$\not 33$	35	37	$\not 39$
41		43	$\not 45$	47	49
$\not 51$		53	55	$\not 57$	59
61		$\not 63$	65	67	$\not 69$
71		73	$\not 75$	77	79
$\not 81$		83	85	$\not 87$	89
91		$\not 93$	95	97	$\not 99$

1.3素数、算数基本定理

对于素数 $p_3 = 5$,

1	2	3		5	
		7			
11		13			
		17		19	
		23			
~~25~~				29	
31					
~~35~~				37	
41		43			
		47		49	
		53			
~~55~~				59	
61					
~~65~~				67	
71		73			
		77		79	
		83			
~~85~~				89	
91					
~~95~~				97	

对于素数 $p_4 = 7$,

1	2	3	5		
		7			
11		13			
		17		19	
		23			
				29	
31					
		37			
41		43			
		47		~~49~~	
		53			
				59	
61					
		67			
71		73			
		~~77~~		79	
		83			
				89	
~~91~~					
		97			

不超过100的素数：

~~1~~	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			

1.3素数、算数基本定理

Mersenne 素数

定理 1.3.6 设 $n>1$是一个正整数，若 a^n-1是素数，则 $a=2,n$是素数。

证明： 若 $a>2$，则 $a^n-1=(a-1)(a^{n-1}+\cdots+a+1)$，而 $1<a-1<a^n-1$，故a^n-1不是素数。与已知矛盾，因此 $a=2$。

若 $a=2$，而 $n=kl,k>1,l>1$ 则

$$2^{kl}-1=(2^k-1)(2^{k(l-1)}+\cdots+2^k+1)$$

而 $1<2^k-1<2^n-1$，故2^n-1不是素数。与已知矛盾，因此 n是素数。

目前，寻找Mersenne素数主要采用计算机搜索的方法，已发现的Mersenne素数有41个。

1.3素数、算数基本定理

截止到2016年1月，GIMPS共搜索到15个梅森素数。现在已知的最大的梅森素数是2016年1月7日发现的2^{74207281}-1，共有22338618位数，此数同时也是已知最大的素数。

2009年，互联网梅森素数大搜索因为第一个发现具至少1,000万个数位的素数，而获得10万美元的奖金。电子前哨基金会亦为具至少1亿个数位及10亿个数位的素数分别提供15万美元及25万美元的奖金。

1.3素数、算数基本定理

Fermat素数

定理1.3.7 若2^n+1是素数，则n一定是2的方幂。

证明： 若n有一个奇素因子q，令$n=qr$，则

$$2^{qr}+1=(2^r+1)(2^{r(q-1)}-2^{r(q-2)}+2^{r(q-3)}+\cdots-2^r+1)$$

而$1<2^r+1<2^n+1$，故2^n+1不是素数。与已知矛盾，因此n一定是2的方幂。

定义1.3.3 形如$F_n=2^{2^n}+1$的数称为Fermat数，当F_n是素数时，称为Fermat素数。

最小的5个Fermat数为 $F_0=3,F_1=5,F_2=17,F_3=257,F_4=65537$

都是素数。因此，Fermat猜测所有的Fermat数都是素数。

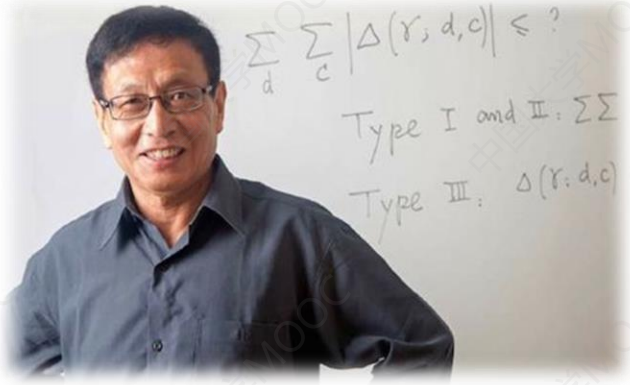
这个猜测并不正确。目前已经证明当$n=5$，6，7，8，9，11，12，18，23，36，38，73时，F_n均不是素数。

拓展

孪生素数：指相差2的素数对，例如3和5，5和7，11和13…。孪生素数猜想正式由希尔伯特在1900年国际数学家大会的报告上第8个问题中提出。

可以这样描述：
存在无穷多个素数p，使得$p+2$是素数。
素数对$(p,p+2)$称为孪生素数。
在1849年，阿尔方·德·波利尼亚克提出了一般的猜想：
对所有自然数k，存在无穷多个素数对$(p,p+2k)$。$k=1$的情况就是孪生素数猜想。

拓展



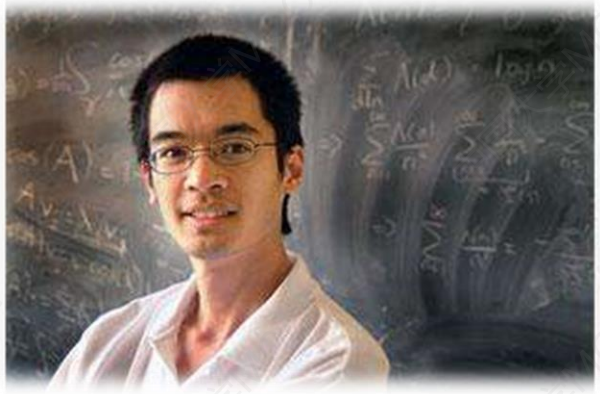
张益唐（1955年—），华人数学家。现在美国加州大学圣塔芭芭拉分校数学系任教 。

张益唐研究的其中一个学术问题通常被称为“素数间隔”。2013年5月，他证明了孪生素数猜想的一个弱化形式，发现存在无穷多差小于7000万的素数对，从而在孪生素数猜想这个此前没有数学家能实质推动的著名问题的道路上迈出了革命性的一大步。

拓展

假如在素数王国里素数只能找邻近的同类结婚，那3、5、7、11这种小素数找对象都很容易。但是素数越大，对象就越难找。但是根据张益唐的发现，素数和下一个素数的距离，应该小于或等于七千万。孤独的数字不会持续孤独下去，总有另一个素数与之匹配。换言之，对于“大龄光棍”素数来说，七千万步之内，必有芳草。

拓展



陶哲轩（1975年-），华裔数学家，任教于美国加州大学洛杉矶分校（UCLA）数学系。

陶哲轩是赢得菲尔兹奖的第一位澳大利亚人，也是继1982年丘成桐之后获此殊荣的第二位华人。

陶哲轩在网络上聚集了世界上一大批数学家开展讨论，很快就将数值降到246

谢谢！