The Colorado State Torus

Edition 2 April 2025

A Glimpse into the World of Möbius Inversions

Tatum Rask

The study of Möbius inversion began with number theory. For now let's focus on a specific example: Euler's totient function $\varphi(n)$ takes as input a positive integer and returns the number of integers m such that $1 \leq m \leq n$ and $\gcd(m, n) = 1$. It turns out that $n = \sum_{d|n} \varphi(d)$. In this case, we call Euler's totient function the **Möbius inverse** of the identity function. The Möbius inversion formula, then, tells us that $\varphi(n) = \sum_{d|n} d \cdot \mu(n/d)$ where μ is given by

$$\mu(z) = \begin{cases} 1 & \text{if } z = 1, \\ (-1)^t & \text{if } z \text{ is a product of} \\ & t \text{ distinct primes}, \\ 0 & \text{if } p^2 | z \text{ for some prime } p. \end{cases}$$

Indeed, for any arithmetic functions f and g such that $g(n) = \sum_{d|n} f(d)$ for $n \in \mathbb{Z}_{>0}$, we also have that $f(n) = \sum_{d|n} g(d)\mu(n/d)$. In our example involving Euler's totient function, $f(n) = \varphi(n)$ and $g(n) = n$.

We can extend this idea to a more general class of posets. Consider a locally finite poset P: that is, P is a partially ordered set where all intervals $[a, b] = \{c \mid a \leq c \leq b\}$ have finitely many elements. Then, consider a real-valued function $f : P \to \mathbb{R}$ (with the property that $f(x) = 0$ whenever $x \leq p$ for some $p \in P$). The **Möbius inverse** of f is given by the (unique) map $\partial f : P \to \mathbb{R}$ satisfying $f(p) = \sum_{q \leq p} \partial f(q)$.

Indeed, f and its Möbius inverse ∂f also satisfy $\partial f(p) = \sum_{q \leq p} f(q)\mu(q, p)$. But what is the function $\mu(q, p)$ in this setting? To understand this, we have to introduce the **incidence algebra** of a poset. The incidence algebra of P is the algebra of all functions $f : P \times P \to \mathbb{R}$ (such that $f(q, p) = 0$ for $q > p$) where addition is point-wise addition and multiplication is convolution. This algebra is not guaranteed to have all inverses, but the function given by $\zeta(q, p) = 1$ for all $q \leq p$ does have an inverse. Its inverse is the **Möbius function** $\mu(p, q)$: that is, $(\zeta * \mu)(q, p) = (\mu * \zeta)(q, p) = 1$ only when $p = q$ (this is the multiplicative identity in the incidence algebra).

The generalization of Möbius inversion to other posets has opened the door for the theory of Möbius functions to be used in various fields of math. If you are an applied topologist, you may know that the persistence diagram is the Möbius inversion of the rank function [1]. If you are a graph theorist, you may know that the chromatic polynomial is the Möbius inversion of the function $x^{\#\text{vertices in S}}$ for graphs S given by contracting edges in G. If you are a network scientist, you may know that counting proper flows on a network is also a Möbius inversion (fun fact - it is essentially the same Möbius inversion as in the case of graph colorings, at least according to Rota [2, Section 10]). Now, think about your own field of research, if I did not mention it above. Are there natural poset structures floating around? What sort of quantities/objects, if any, can be interpreted as a Möbius inversion? I encourage you to think about these questions and utilize the vast theory of Möbius functions!

[1] Amit Patel. Generalized persistence diagrams. *Journal of Applied and Computational Topology*, 1(3):397–419, June 2018.

[2] Gian-Carlo Rota. On the foundations of combinatorial theory I. Theory of Möbius Functions. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 2(4):340–368, 1964.

Growing Food Security

Growing Food Security *is a graduate student-led project that grows fresh produce for the Rams Against Hunger Food Pantry at CSU. Each year, we grow and donate* ***over 10,000 pounds of fruits and vegetables****, helping promote food security on campus. Volunteering with us is a* ***great way to meet new people in the CSU community, gain hands-on experience in growing healthy food, and make a tangible impact*** *in our community. No prior experience is needed, and all commitment levels are welcome! Plus, volunteers get* ***free access to fresh produce****. To be added to our mailing list, contact Tatum Rask at tatum.rask@colostate.edu*

Problem of the Month

Consider the sum

$$77 + 757 + 7557 + 7\overbrace{5\ldots5}^{98}7 = \frac{7\overbrace{5\ldots5}^{99}7 + m}{n}$$

Here, $n, m < 3000$. Find $m + n$

The answer will be included in next month's edition. Submit your solutions to **MATH_ColoradoStateTorus@mail.colostate.edu** for bragging rights.

Congratulations to **Michael Moy** for being the first to solve the March Problem of the Month!

Want to learn to dance for free with Ignacio?

I'm preparing to teach a dance class next semester, and as part of the process, I'm auditioning at the Rec Center. I need volunteers for a fun, 20 min mock class! No experience needed, I like to say the only requirement needed to learn to dance is not knowing how to dance*! Faculty, students, and anyone are welcome.*

- ***When?*** *Sometime between* ***April 15th and 17th*** *(exact time TBD).*
- ***Where?*** *CSU Rec Center.*
- ***Interested?*** *Message me via phone (9708898979) or email (ir@colostate.edu), and I'll keep you posted on the details! Come dance, have fun, and help me out in the process!*

Trouble at the limits of equality

James B. Wilson

Confusion at the limits of infinity has researchers concerned that equality itself may not be sound.

Today's equals follows Leibniz's work to unify the Euclidean *congruence* in geometry and Al Khawarismi's *balance* in algebra. (Algebra was story problems speaking of "balancing" substances). Leibniz proposed equality is permission to interchange objects without effect:

$$x = y \implies (\forall P)(P(x) \Leftrightarrow P(y))$$

However, this did nothing to explain what makes two objects equal in the first place, outside of the *reflexive law:* $x = x$, which has no interesting uses.

Frege hoped to define equals in terms of Cantor's newly invented *sets*, but he got lost in vague stories, arguing that the morning star and the evening star are equal as they are both the planet Venus; so, some differences should not count. Eventually Zermelo did capture Frege's idea. He required that the only property that can be spoken about sets must be of the form $P(u, v) \equiv$ Is $u \in v$?. So the Leibniz Law becomes:

$$x = y \quad \Longrightarrow \quad (\forall z)(z \in x \Leftrightarrow z \in y).$$

Zermelo thus took the converse as his first axiom of axiomatic sets and we know it today as "2-way set containment".

The Frege-Zermelo option was an immediately unconvincing solution as it was not even objectively reflexive, e.g. the number 2 could be represented as an axiomatic set as $\{\{\{\}\}\}$ and $\{\{\}, \{\{\}\}\}$ but those sets are not equal in the Zermelo set theory. Bourbaki proved that Zermelo sets are rigid rooted trees with finite depth branches; so, Zermelo equality is merely a disguised reflexive law.

Since the 1950's researchers Lawvere, Martin-Löf, Awodey, Voevodsky, and others have been working on a new approach to equality based on category theory. The idea is that equality comes in layers. E.g. $\{\{\{\}\}\} \neq \{\{\}, \{\{\}\}\}$ but if you decide that each should encode the number 2 then you should think of this as introducing a rewriting rule of the symbols. Thus, equality can hold complexity beyond the reflexive law which we exploit with equations. To prove this is sound the plan is to work inductively through layers of added equality complexity, using equality itself as the induction counter. That is,

$$x \equiv y \qquad := \qquad (x = y) = (x = y).$$

For example, we might say $(2 = 2) \neq (\{\{\{\}\}\} = \{\{\}, \{\{\}\}\})$ even though both speak of the same concept, because $2 = 2$ is founded on the reflexive law while the right-hand-side is a mindful addition of rewriting rule. This layering of equality has been modeled in homotopy theory and the interplay has lead to an explosion of recent progress.

Now to the trouble. When we continue the process we get equality of equalities of equalities. Each adds their layer to the equal sign. But there are many versions of ∞-categories to use as the limit of this process and so the final version of equality does not appear to be well-defined!

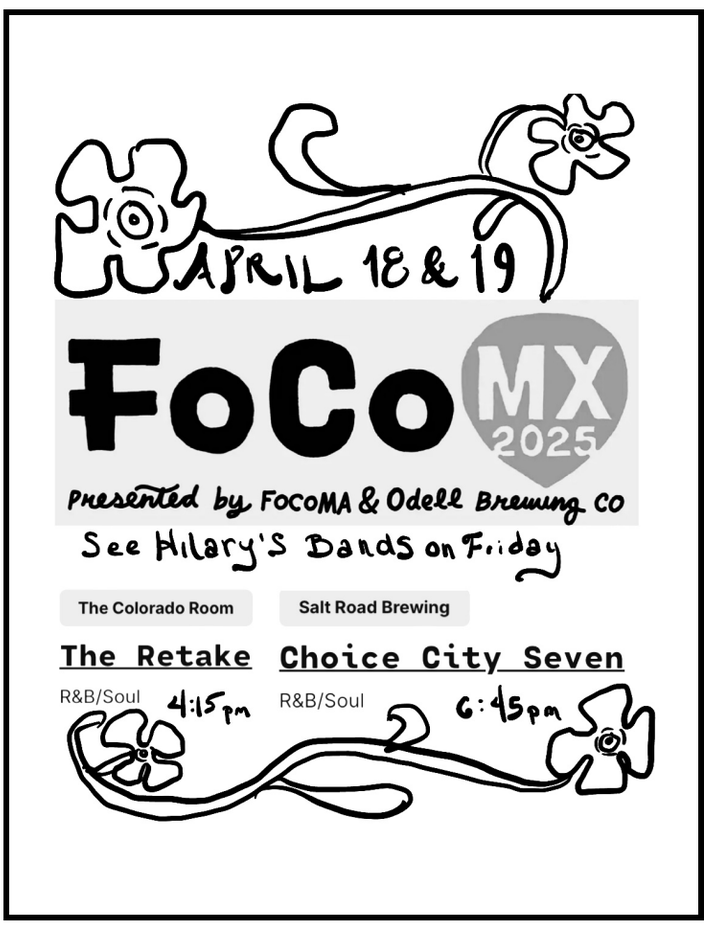
We can see this from the following optical calculation.

$$1 = 1 = 1 \quad 1 = 1 \equiv 1 \quad 1 = 1 \equiv 1, \ldots$$

Take the limit of adding dashes to equals and it fills in to a large minus sign where we compute:

$$1 = 1 \blacksquare 1 = 0.$$

Of course this last sentence is an April Fool's joke, but *everything* up to that line is true and a warning that one day soon you might see the real headline that equality as you think of it is wrong. For now just know that it is undefined.



Distinguished Professor Ingrid Daubechies to Speak at CSU
Arne Magnus Lecture Series

Public Lecture & Reception

Thursday 4/17 4pm Lory Student Center, University Ballroom/Lounge
"Mathematicians Helping Art Conservators and Art Historians"

Colloquium

Friday 4/18 10am Weber 237
"Discovering Low-dimensional Manifolds in High-dimensional Data"

Not all Polynomials are Created Equal

Ian Jorquera

There are a lot of named classes of polynomials out there, each class serving various mysterious purposes. My research has recently lead me to be interested in Conway polynomials. My recent research has been focused on the structure of equiangular systems of lines over finite fields, and I often find myself computing different examples over different finite fields using my impromptu python scripts. And so, I have been rather interested in the different methods used to efficiently compute over finite fields, which lead me to Conway polynomials.

A finite field of a prime power p^n elements, denoted $\mathbb{F}_{p^n}$ is constructed by adjoining a root of an irreducible polynomial of degree n, with the base field $\mathbb{F}_p$. For example to construct $\mathbb{F}_9$ we could consider the degree 2 polynomial $x^2 - 2$ which is irreducible as a polynomial over $\mathbb{F}_3$. In this case a root α of this polynomial would satisfy $\alpha^2 = 2$, meaning it would behave like the square root of 2. Adjoining this root with the base field would give us $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ whose elements would look like $a\alpha+b$ where $a, b \in \mathbb{F}_3$ along with the relation $\alpha^2 = 2$. From this we can see that multiplication in finite fields is basically just multiplication of polynomials, which can be rather costly in large computations.

But there is a better way! Because the multiplicative group of a finite field is cyclic, if we were able to find a multiplicative generator $\omega \in \mathbb{F}_{p^n}$ we could represent any elements $x, y \in \mathbb{F}_{p^n}$ as powers of the generator: $x = \omega^k$ and $y = \omega^\ell$ and multiplication then becomes no more difficult then addition: $xy = \omega^k\omega^\ell = \omega^{k+\ell}$. But the hard part here is finding a multiplicative generator! Enter the Conway polynomials, which is a class of polynomials depending on p and n, which are irreducible, and whose roots can be used as multiplicative generators of the field $\mathbb{F}_{p^n}$. For $p = 3$ and $n = 2$ the Conway polynomial is $x^2 + 2x + 2$, and a root α when adjoined with the base field gives us a very nice representation of $\mathbb{F}_9 = \mathbb{F}_3(\alpha) = \mathbb{F}_3[x]/(x^2+2x+2)$ where α is a multiplicative generator. Don't believe me? Try it out your self.

In general there are many different polynomials that satisfy these requirements, so a Conway polynomial $C_{p,n}$ is generally defined to be the "minimal" such polynomial up to some non-canonical lexicographical order on the polynomials in $\mathbb{F}_p[x]$, that are also compatible with all Conway

polynomials $C_{p,m}$ for all degrees m dividing n. These additional restrictions help reduce the search space for Conway polynomials by orders of magnitude. The only issue, is that we have really only pushed the goal post from finding multiplicative generators to Conway polynomials. Luckily for me, there are large tables of known Conway polynomial for the primes p and degrees n I have needed so far, and hopefully I won't need to venture outside of these tables of known Conway polynomials. But luckily for us, there are also algorithms to generate these polynomials that beat a simple brute force search.

Foto del Mes

This month's photo is from Visit Day! Thanks to Ignacio for the photo.

Seminars

- *Applied Category Theory Seminar (ACTS)*
  Weber 237, Thursdays 4-5pm
  contact: nathaniel.collins@colostate.edu
- *Codes and Expansions (CodEx)*
  Online only, Tuesdays 11am
  math.colostate.edu/∼king/codex
- *Greenslopes (Graduate Students Only)*
  Weber 201, Thursdays 11am
  contact: ashley.armbruster@colostate.edu
- *IDA Seminar*
  Weber 223, Thursdays 3-4pm
  contact: jennifer.l.mueller@colostate.edu
- *Math Ed Seminar*
  Weber 15, Tuesdays 11-12am
  contact: hortensia.soto@colostate.edu
- *MMaRgs/Fragment*
  Weber 201, Thursdays 3-4pm
  contact: mark.shoemaker@colostate.edu
- *Number Theory Lab*
  Weber 223, Thursdays 12pm
  contact: cigole.thomas@colostate.edu
- *Pattern Analysis Lab (PAL)*
  Weber 11, Wednesdays 3-4pm
  contact: michael.kirby@colostate.edu
- *RMAC*
  Weber 223, Fridays 4-6pm
  contact: james.wilson@colostate.edu
- *Matemáticas*
  Weber 15, Mondays 4-5pm
  contact: jake.kettinger@colostate.edu

Dean, Beans, & a Burrito Breakfast

The next Burrito Day is at 8:30-9:30am on April 8th in the new GradSpace, in the General Services building, room 203.

March Problem of the Month Solution

Find all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(2x) + 2f(y) = f(f(x+y))$ for all $x, y \in \mathbb{Z}$

Solution: Claim: if $f \neq 0$, then f is a linear function. Reason: Plug in $(0, n)$ and $(1, n-1)$ for (x, y). We get:

$$\begin{aligned} f(0) + 2f(n) &= f(f(n)) \\ &= f(1) + 2f(n-1) \\ &\Longrightarrow \\ f(n) - f(n-1) &= \frac{f(1) - f(0)}{2} \end{aligned}$$

This difference is constant for all such n. So $f(x) = ax + b$ for some $a, b \in \mathbb{Z}$. Then:

$$\begin{aligned} 2f(n) &= 2an + 2b \\ f(2m) &= 2am + b \\ f(2m) + 2f(n) &= 2am + 2an + 3b \\ f(f(m+n)) &= f(am + an + b) \\ &= a^2 m_a^2 n + (a+1)b \end{aligned}$$

Hence,

$$\begin{aligned} f(2m) + 2f(n) &= f(f(m+n)) \\ &\Longleftrightarrow \\ 2am + 2an + 3b &= a^2 m + a^2 n + (a+1)b \end{aligned}$$

Comparing the coefficients, we see that $2a = a^2$ and $3 = a + 1$, so $a = 2$ and $b \in \mathbb{Z}$ has no constraints. Thus

$$\{f_b(x) = 2x + b : b \in \mathbb{Z}\} \bigcup \{f = 0\}$$

is the family of solutions.

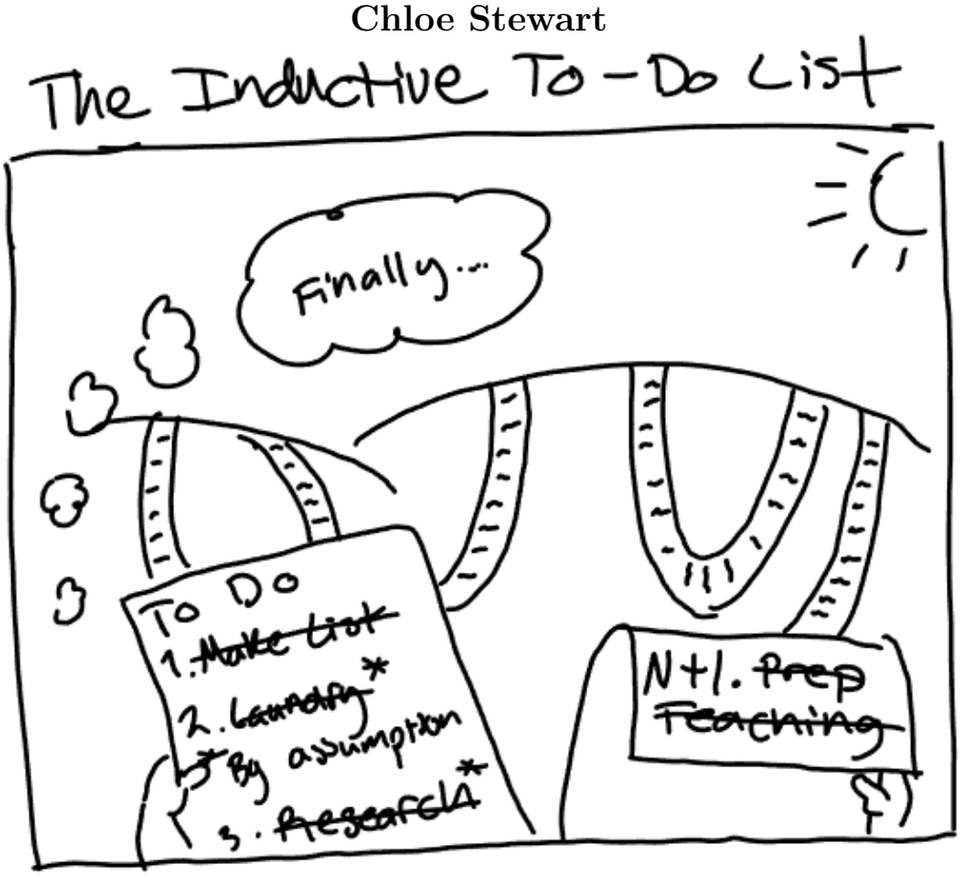
SIAM will host a trip to Cheyenne, WY on Tuesday, April 8 to visit the NCAR-Wyoming Supercomputing Center (NWSC) which houses advanced computing and data storage resources for research in the Earth system sciences. The tour will take place from 1-3pm. We will plan to leave campus by 11:30 and be back around 4pm.

Call to Contribute

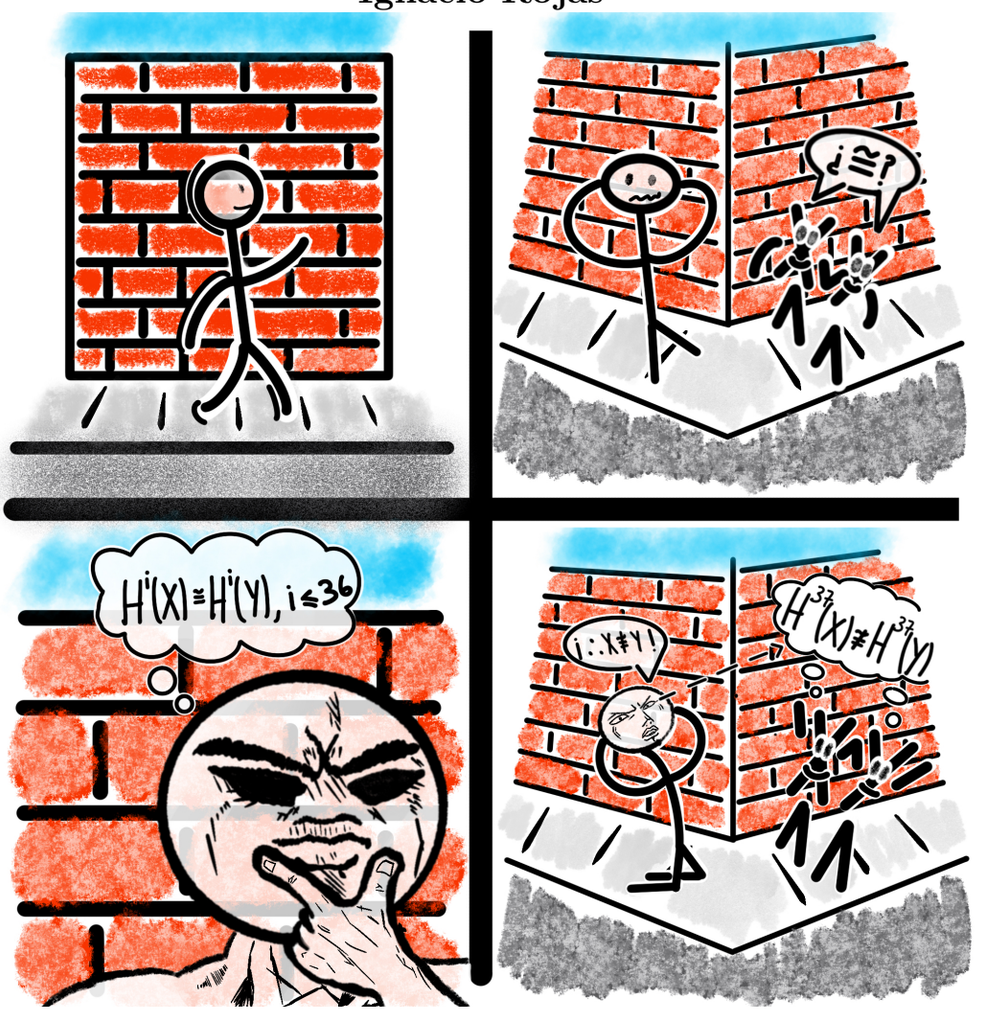
We hope you have enjoyed the Second edition of The Colorado State Torus. Do you have any ideas for articles, opinion pieces, or new sections? Do you have an error to point out in a seminar time? Just want to give us a piece of your mind? We would love to hear from you! The CST is made possible through contributions from many people across the department. Send any articles, comics, suggestions, announcements, ads, or anything you wish to be included to **MATH_ColoradoStateTorus@mail.colostate.edu** at least one week before the end of the month. The editorial board will review any ideas and hopefully include them in an upcoming issue. Thank you!

April Comics

Chloe Stewart



Ignacio Rojas



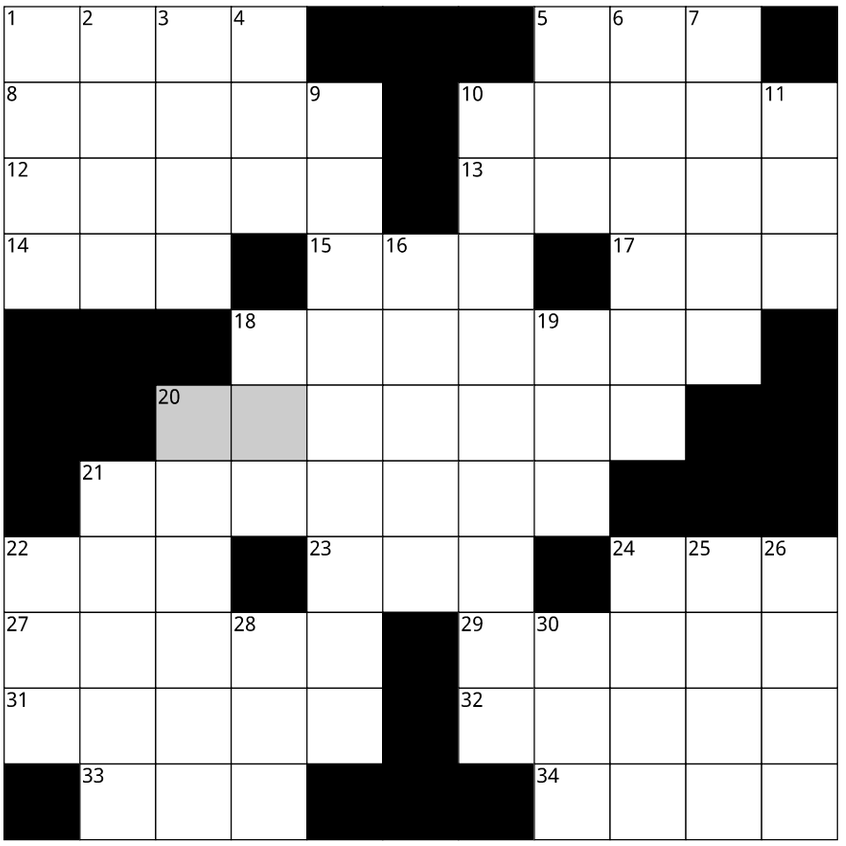
April Issue Crossword

ACROSS

1 Start of a play
5 Blind mammal
8 A major, for example
10 Task with an April deadline
12 Thanks, in France
13 Rear
14 Lamb's mother
15 Hot tub
17 Nonprescription, for short
18 College
20 "April ___ bring May ___ "
21 Neighbor of Tennessee
22 Holiday prelude
23 One ___ time
24 Prefix with gram
27 Display
29 Scouting job
31 Magical rune
32 Massage
33 Bear's home
34 Hello, in Sydney

DOWN

1 Highest level
2 Gnaw
3 Burned rubber
4 U.S. payment law, abbr.
5 Sound made by a 14-across
6 Mathematical postulates
7 Irritated
9 Center of many a dancefloor
10 Corporate symbol
11 "One ___, please"
16 Beg, as a dog
18 "Eureka!", or in the style of
19 Historical period
20 Hammer, or provide with feathers
21 Skirt
22 Ambulance letters
24 Made no mistakes
25 Weather agency
26 Former grad student of Renzo
28 German article
30 H.S. subject



March Solutions